

SUSPECT UNTIL PROVEN GUILTY

A PROBLEMATIZATION OF STATE DOSSIER SYSTEMS VIA TWO CASE STUDIES:

THE UNITED STATES AND CHINA

Kenneth N. Farrall

A DISSERTATION

in

Communication

Presented to the Faculties of the University of Pennsylvania

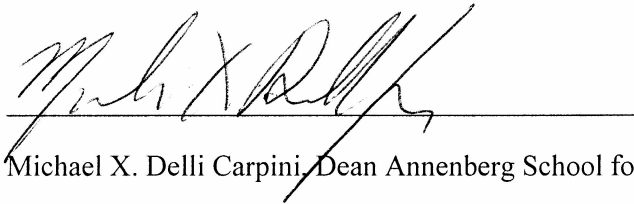
in

Partial Fulfillment of the Requirements for the

Degree of Doctor of Philosophy

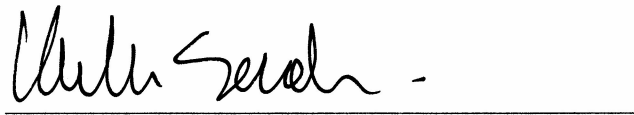
2009

Supervisor (or co-Supervisors) of Dissertation

A handwritten signature in black ink, appearing to read "Michael X. Delli Carpini", written over a horizontal line.

Michael X. Delli Carpini, Dean Annenberg School for Communication

Graduate Group Chairperson

A handwritten signature in black ink, appearing to read "Katherine Sender", written over a horizontal line.

Katherine Sender, Associate Professor of Communication

Dissertation Committee

Oscar H. Gandy, Jr., Professor emeritus

Klaus Krippendorff, Gregory Bateson Professor of Communication

Joseph Turow, Robert Lewis Shayon Professor of Communication

## DEDICATION

This dissertation is dedicated to my wife, Dong, whose support and patience gave me the strength, and our three children Myles, Eric and Kathryn, who gave me the inspiration to see this project through to its completion.

## ACKNOWLEDGEMENTS

Thank you, Oscar Gandy, for sparking my interest in privacy and surveillance and continuing to support my work even after your (much too early) retirement. Your support kept me moving forward, especially during the difficult times. I have been truly honored to have you as a friend and mentor.

Thank you, Klaus Krippendorff, for introducing me to the power of language and the world of cybernetics, and for opening my mind to ways of thinking that will serve me for the rest of my life.

Thank you, Joseph Turow, for instilling in me a much deeper appreciation for the importance of substance over theory.

Thank you, Michael Delli Carpini, for your friendship, your guidance, and your inestimable capacity to turn problems into solutions.

A special thank you to Monroe Price, for recharging my interest in international communication, and the material support that made it possible for me to pursue that interest.

Thank you, to my friends and colleagues at the Annenberg School, some of the finest people I have ever known. Thank you to Josh Lauer, Jennifer Horner, Deb Lubken, Bill Herman, Zhan Li, Chris Finlay, and Lokman Tsui for their advice and friendship over the years.

Thank you to Annenberg's wonderful support staff, especially Bev Henry, Deb Porter, Sharon Black, Rich Cardona, Lizz Cooper, and Joanne Murray.

Finally, to my parents, George and Judy Farrall, to whom I will forever be indebted, this would never have been possible without you.

# ABSTRACT

## SUSPECT UNTIL PROVEN GUILTY

### A PROBLEMATIZATION OF STATE DOSSIER SYSTEMS VIA TWO CASE STUDIES:

### THE UNITED STATES AND CHINA

Kenneth N. Farrall

Michael X. Delli Carpini  
Dissertation Supervisor

This dissertation problematizes the “state dossier system” (SDS): the production and accumulation of personal information on citizen subjects exceeding the reasonable bounds of risk management. SDS — comprising interconnecting subsystems of records and identification — damage individual autonomy and self-determination, impacting not only human rights, but also the viability of the social system. The research, a hybrid of case-study and cross-national comparison, was guided in part by a theoretical model of four primary SDS driving forces: technology, political economy, law and public sentiment. Data sources included government documents, academic texts, investigative journalism, NGO reports and industry white papers. The primary analytical instrument was the juxtaposition of two individual cases: the U.S. and China. Research found that constraints on the extent of the U.S. SDS today may not be significantly different from China’s, a system undergoing significant change amidst growing public interest in privacy and anonymity. Much activity within the U.S., such as the practice of suspicious activity reporting, is taking place outside the domain of federal privacy laws, while ID systems appear to advance and expand despite clear public opposition. Momentum for increasingly comprehensive SDS appears to be growing, in part because the harms may not be immediately evident to the data

subjects. The future of SDS globally will depend on an informed and active public; law and policy will need to adjust to better regulate the production and storage of personal information. To that end, the dissertation offers a general model and linguistic toolkit for the further analysis of SDS.

## TABLE OF CONTENTS

LIST OF TABLES	vii
LIST OF ILLUSTRATIONS	viii
CHAPTER 1: Surveillance as a Social Problem	1
CHAPTER 2: Problematizing the State Dossier System	26
CHAPTER 3: U.S. Case, historical context	87
CHAPTER 4: U.S. Case	122
CHAPTER 5: Privacy across Cultures	202
CHAPTER 6: China Case	231
CHAPTER 7: Synthesis	286
APPENDIX A: Searching for the Mother of All Databases (research note)	326
APPENDIX B: Document Source Breakdown	334
REFERENCES:	336

## LIST OF TABLES

Table 1. Case Nodes and Data Sources.....	85
Table 2. Claims and Data Sources.....	312

## LIST OF ILLUSTRATIONS

Figure 1. Document Retrieval Cycle	77
Figure 2. SIP Snowball, U.S. Case	79
Figure 3. Data Triangulation	82
Figure 4. SAR Information Flow Diagram	176
Figure 5. Linguistic Juxtaposition	202
Figure 6. Privacy	204
Figure 7. Public-Private	215
Figure 8. Anonymity	221
Figure 9. Data Shadows Through Time	245
Figure 10. Information Creation and Available Storage	290
Figure 11. Linguistic Toolkit	299
Figure 12. SDS General Model	300
Figure 13. Production: Site and Logic	301
Figure 14. The Targeted Person	310
Figure 15. Multidimensional Comparison of U.S. and China Surveillance	315
Figure 16. SIP Snowball Detail, U.S. Case	327



## CHAPTER 1: SURVEILLANCE AS A SOCIAL PROBLEM

This dissertation “problematizes” a particular domain of surveillance practice I call the “state dossier system.” This phrase is not intended to be normatively neutral, but to diagnose a social problem. At appropriate times neutral terms such as “information system,” database, and record will be used, but the goal of this work is to illuminate and contribute to the further analysis and regulation of what may be the single most important threat of states to the public interest this century: the unconstrained production and accumulation of personal information on state subjects that exceeds the reasonable bounds of the state’s mandate to manage risk.

The concept of problematization, notes Foucault (1985) is “an ‘answer’ to a concrete situation which is real” (p. 115).<sup>1</sup> Key to the problematization is the language that is used and developed — specific terms and concepts which help illuminate the relevant elements of the problem. The problematization of madness, for example, was built upon words like “mania” and “melancholia.” A problematization is not a theory per se. It is not intended to create a definitive model with predictive power, but to highlight key aspects of a real world problem, that, once properly identified, may be amenable to management and regulation.

As the scope and depth of a state dossier system grows, the interface between the state and its subjects tends to grow more tense and unfriendly. An increasing number of citizens fall under clouds of suspicion that tend to hang over them throughout their lives; they are “suspect until proven guilty.” State dossier systems damage individual autonomy and self-determination, impacting not only the human rights of the subject population, but also the overall ability of that social system to adapt to change.

---

<sup>1</sup> Problematization is described in more detail later in the chapter.

The dossier system is a particular state practice that falls within the more general definition of surveillance. By focusing on the term “state dossier system” rather than “state surveillance,” I avoid the conflation of necessary state information practices with those that are specifically harmful to the public interest.<sup>2</sup> Nevertheless, extant “surveillance theory” will be drawn upon frequently in the course of this analysis.

The primary analytical instrument for this problematization is the juxtaposition of two individual cases of state dossier systems: the U.S. and China. It is important to note that the two cases are not given equal weight in either the data set or the subsequent analysis. The U.S. case is the focal case, while the China case serves more of an instrumental role which can be broken down into two primary functions: 1) the China case serves as yardstick for assessing the severity of the U.S. state dossier problem; and 2) the consideration of dossier practices within what are generally understood to be highly contrasting social systems affords the efficient development of generalized terms and concepts that one can expect to apply to a wide range of state dossier cases. This is not to diminish the intrinsic importance of the China case. The U.S. case, however, is in many ways more complex and less well understood than China. The Chinese surveillance and dossier systems have already been problematized within western academia and popular discourse to such a degree that it would be more difficult to make significant contributions in this area. We will see, however, that assumptions about the authoritarian nature of the Chinese state and the intensity of the dossier system (ID and personal record systems) do not always hold up under

---

<sup>2</sup> Napoli (2001) distinguishes between three different conceptualizations of the term “public interest:” *majoritarian*, *procedural* and *unitary*. The majoritarian approach assumes that the public interest is served when the interests of a majority of people are met, regardless of how the rest might be impacted. The procedural definition is almost tautological — that the public interest is whatever the policy process concludes is in the public interest. Finally, the unitary approach, which I adopt here, assumes that the public interest has a normative definition, and that such a definition comprises a set of guiding principles. Although these principles are assumed to be held in high regard by the average person, they must be articulated within a particular policy context if they are to have any force. In the context of media ownership, diversity has become a core principle that policy makers publicly support, although their strategies for achieving this principle may be highly divergent. The guiding principles that inform the public interest in the context of state surveillance are self determination, autonomy and freedom of expression — key to any functioning democracy. I elaborate on this point in chapter 2.

scrutiny. There is more life to the public as an opposition force to the states authority than many acknowledge.

This chapter's primary goal is to orient the reader to the broader literature that approaches surveillance as a social problem and examine some of the most common choices of language and framing that drive them. The chapter is divided into five sections: *Global Surveillance as a Social Problem* introduces the general concept of surveillance as a "social problem" and its apparent relentless growth and expansion worldwide; *Problems, Frames, and Social Change* examines the role of language and social change within the context of surveillance studies; *Definitions and Theoretical review* elaborates upon the notion of "problematization" and its relationship to theory, defines surveillance and reviews the major strands of surveillance theory; *Popular Surveillance Problem Frames* identifies and critiques popular problem frames that frequently appear within the "surveillance studies" literature; finally, *Plan of Dissertation* outlines the essence and rationale for the six subsequent chapters.

## GLOBAL SURVEILLANCE AS A SOCIAL PROBLEM

It is fair to say that in the years since September 11<sup>th</sup>, 2001, the issue of surveillance, the systematic production or capture of information about people, processes and institutions that is then integrated into schema for social action, has become particularly salient in public discourse. Anthony Giddens (1985) and Michel Foucault (1979) have helped us to understand that surveillance plays a critical regulatory role in any complex social system. The emerging sub-discipline "surveillance studies," however, has called our attention to the intensification of surveillance worldwide and its negative impact on human rights, privacy and self-determination (Gandy, 1993; Lyon, 2001; Ball & Webster, 2003; Marx, 2002; Monahan, 2006).

Despite the growing volume of academic texts defending the right to privacy for individuals and groups, the scope of global surveillance systems continues to expand along with the depth of personal information they record and store. The ACLU's "The Surveillance-Industrial Complex: How the American Government Is Conscribing Businesses and Individuals in the Construction of a Surveillance Society" (Stanley, 2004) details how U.S. government surveillance practices have come to rely on a multi-billion dollar industry led by private data aggregators Acxiom and Choicepoint, and how this moves many surveillance practices outside the realm of privacy law. The Privacy Act of 1974, for example, prevented state law enforcement from maintaining information on citizens who were not the subject of investigation. Not only are private corporations exempt from this distinction, but there are no legal restrictions on the government for using this information or presenting it as evidence in a court of law. Further, the report details how data gathered by companies on their customers in the normal course of business — flight records, credit card reports, phone logs, email — are often freely provided to the government upon request. For those companies that do resist, the state has made increasing use of the "National Security Letter" to compel companies to release data.

The International Campaign Against Mass Surveillance (ICAMS) 2005 report, "The Emergence of A Global Infrastructure for Mass Registration and Surveillance" goes beyond the U.S.-centered context of the ACLU report, detailing how, since September 11<sup>th</sup>, once substantial nation-state to nation-state boundaries in surveillance formations have been dissolving as the states become embedded in a "global infrastructure:"

The result has been an emerging trend toward the harmonization and integration of security functions on a global scale. In democratic countries, this has led to a rollback of rights, freedoms, and civil liberties that have been won by centuries of popular struggle. In undemocratic countries, repressive regimes have been enabled and strengthened, and development assistance has been diverted to bolster security apparatuses. Internationally, the post-World War II order — which enshrines the universal, inalienable human rights of all individuals — has been seriously eroded. (p. 7)

The literature on surveillance today appears overwhelmingly weighted to the inevitability of increasingly expanding surveillance regimes across the globe (Hunter, 2002; O’Harrow, 2006). For political economists, there seems to be something built into the logic of global capitalism and the instrumental rationality of bureaucracy that drives the expansion of monitoring, cataloging, and data storage and retrieval systems (Gandy, 1993; Robins & Webster, 1999). For technology scholars, the incessant growth in computer processing, storage and network bandwidth capacity vastly expands the possibilities for surveillance, possibilities which human actors inevitably begin to make use of (Winner, 1978; Lyon, 2002; Marx, 2002). Although these long term political economic and technological factors have been driving the growth of state surveillance for quite some time, a single geopolitical event, the September 11<sup>th</sup> terrorist attacks, appears to have precipitated a “perfect storm” of state surveillance. A range of formerly effective social constraints are rapidly losing their relevance and force, while state surveillance systems across the globe become more all encompassing and centralized (“International Campaign Against Mass Surveillance (ICAMS),” 2005).

This new, fuzzy threat of terrorism is now increasingly used to justify a dramatic change in not just the intensity of surveillance but the architecture of global data flows. The failure of the U.S. government to properly anticipate and “manage” the attacks has been blamed on a lack of centralized intelligence powers and the presence of too many institutional boundaries. In a contemporary social environment in which many citizens value their security over their privacy and see increased surveillance as a practical necessity, there has been little public resistance to a series of laws which only begin with the Patriot Act, and include the Real ID Act, the Military Commissions Act (MCA) and ongoing revisions to the FISA Act, which are either rolling back or eliminating prior legal constraints on state surveillance, many in place since the 1970s. Further, legal boundaries that have protected citizens from state surveillance — namely the Privacy Act of

1974 and the Fourth Amendment — have been rapidly losing their relevance (Sundstrom, 1998; “Privacy’s Gap,” 2003; Ko, 2004; Solove, 2006).

## PROBLEM FRAMES AND SOCIAL CHANGE

Ball and Haggerty (2005) have suggested that scholars within the sub-discipline of surveillance studies may have inadvertently contributed to a sense of helplessness in the face of the global expansion of the surveillance grid.

As a group we tend to produce a cumulative image of the inevitable expansion of surveillance and cooptation of efforts to resist surveillance systems. Hence, rather than motivating political action an unintended consequence of how we typically present our accounts might be to induce in the public a form of resigned fatalism and political paralysis. (p. 136)

The specific presentation of accounts of the surveillance problem that Ball and Haggerty refer to here can be classified in terms of their “frames,” or particular uses of language that interpret or highlight a problem in a certain way. As Bennett (2008) reminds us, “[for] any group that seeks to change public policy, or indeed the structural conditions that give rise to that policy, how issues get ‘framed’ is crucial” (p. 1).

The term “frame”, originating in the work of Erving Goffman, is generally understood to mean the use of language that interprets and highlights a problem in a specific way. Snow and Benford (1992) describe a frame as an

interpretive schemata that simplifies and condenses the “world out there” by selectively punctuating and encoding objects, situations, events, experiences, and sequences of actions within one’s present or past environment (p. 137)

Entman (1993) notes that the purpose of a frame is to “select some aspects of a perceived reality and make them more salient in a communicating text” (p. 52) in order to promote a particular way of defining a problem, its cause, and a potential solution. Further, Tarrow (1994) reminds us that:

Social movements are deeply involved in the work of “naming” grievances, connecting them to other grievances and constructing larger frames of meaning that will resonate with a population’s cultural predispositions and communicate a uniform message to power holders and others.

Although not always in the forefront of discussion about frames, the use of metaphor, or the “understanding and experiencing of one kind of thing in terms of another” (Lakoff & Johnson, 1980) can play a major role in the framing of social problems. Schon (1979) argues that “the framing of problems often depends upon metaphors underlying the stories which generate problem setting and set the direction of problem solving” (p. 138). Metaphors may become so established within a particular discourse on a social problem that their presence is hardly noticed (Deignan, 2005).

In his highly influential work, *Contingency, Irony, and Solidarity*, Rorty (1989) deftly describes the contingent nature of the language we use and the futility of asserting the existence of some independent reality beyond words. The words we use facilitate other words and particular frames which become intertwined with and help to stabilize specific conceptual models and forms of practice. According to Rortian pragmatism, changing these words is a critical first step in changing social practice.

What the Romantics expressed as the claim that imagination, rather than reason, is the central human faculty was the realization that a talent for speaking differently, rather than for arguing well, is the chief instrument of cultural change. What political utopians since the French Revolution have sensed is not that an enduring, substratal human nature has been suppressed or repressed by “unnatural” or “irrational” social institutions but rather that changing languages and other social practices may produce human beings of a sort that never before existed. (Rorty, 1989, p.7)

New uses of language can help constitute new social opportunity spaces and offer innovative concepts that promote the solution of problems. The use of new language does not necessarily equate to the development of formal theory, however. When active language hardens into theory, especially successful ones, human subjects of the theory can begin to lose some of their self-determination.

Politically, the more territory a theory covers, the more it is preferred, the better it will be remembered, and the more likely it will be applied. Thus, theorizing supports a conceptual imperialism; the urge to oversee, predict, control, and govern ever-growing territories....

The requirement that theories be both rational and consistent thus reduces them to monological constructions in the dual sense of being the product of a single voice and of being cast in terms of one (coherent) logic. This has considerable implications for social theorizing. (Krippendorff, 1993, pp. 4-5)

Not only can the imposition of an overarching explanatory logic contribute to a kind of conceptual imperialism, but it can also interfere with and otherwise constrain a scholar's ability to perceive important subtleties of individual real-world cases. In domains of high complexity and rapid change, all-encompassing theories can inhibit understanding:

... surveillance and privacy are part of a bigger picture. They are embedded in the construction of identity, political culture, the practices of everyday life, and in forms of power and resistance. It is dangerous both intellectually and politically to abstract them from the totality of concrete experience.... It is surely valuable to make theories of privacy (e.g., Schoeman 1984), but after a certain point these theories can become misleading unless they incorporate a substantive analysis of historically specific formations of institutionally organized embodied activity. (Agre, 1999, p. 9)

... the quest for an abstract grand theory of surveillance is a wild-goose chase, particularly if it is yoked with particular concepts and is supposed to have universal relevance. The theoretical task is better seen as an ongoing conversation in which concepts and theorems that prove helpful should be explored and used, but even if they loom large they should not be permitted to dominate the debate. (Lyon, 2007a, pp. 46-7)

## DEFINITIONS AND THEORETICAL REVIEW

### PROBLEMATIZATION

The goal of this dissertation is not to develop a comprehensive theory of state dossier systems, but to “problematize” the concept of the state dossier system. I define this term following Foucault:

Some people have interpreted this type of analysis as a form of “historical idealism”, but I think that such an analysis is completely different. For when I say that I am studying the “problematization” of madness, crime, or sexuality, it is not a way of denying the reality of such phenomena. On the contrary, I have tried to show that it was precisely some real existent in the world which was the target of social regulation at a given moment. The



question I raise is this one: how and why were very different things in the world gathered together, characterized, analyzed, and treated as, for example, “mental illness”? What are the elements which are relevant for a given “problematization”? And even if I won’t say that what is characterized as “schizophrenia” corresponds to something real in the world, this has nothing to do with idealism. For I think there is a relation between the thing which is problematized and the process of problematization. The problematization is an “answer” to a concrete situation which is real. (Foucault, 1985, n.p.)

Foucault considered problematization in two ways. The first, which characterized a great deal of his work, was as something in one’s history that can be studied, a discursive process which has left traces of its evolution in texts. The second is simply a realization that problematization is a reaction to a concrete situation out in the world, a strategy that affords the target problem’s regulation. This dissertation is a problematization in Foucault’s second sense, but it is also not without its historical roots. Previous scholars including Donner (1980) and Laudon (1986) have focused on the problematic of unmonitored, unchecked state aggregation of personal information on citizens without criminal records. Solove (2004) has brought our attention to the important role of electronic communication technology in affording “digital dossiers” and their impact on information privacy, autonomy and self-determination. Nevertheless, there is a tendency to dismiss the role of the state or at least minimize it in comparison to the more general problem of surveillance by public and private institutions alike.

The focal tool in the process of problematization is language; problematization comprises a collection of related terms used to speak to the problem. In this dissertation, most of these terms have well established meanings within the relevant literature; others are commonly used but their specific meaning is under some dispute; still others have emerged as part of the exploration and require more explicit definition. The goal, again, is not to end up with a general model that has predictive power, but to focus our thinking on emergent, increasingly significant state practices that endanger the public interest.

To properly situate this problematization of state dossier systems within the larger literature of surveillance studies, I will now offer an explicit definition of surveillance, review the main strands of surveillance theory, and critique popular frames for surveillance problematizations that appear frequently in the literature.

#### DEFINING SURVEILLANCE

Surveillance, according to Ball & Webster (2003), involves the “observation, recording and categorization of information about people, processes, and institutions.” Lyon (2004) offers a definition of surveillance that is similar to Ball & Webster’s, but with an important addition. According to Lyon, surveillance involves the “rationalized control of information within modern organizations, and involves in particular processing personal data for the purposes of influence, management, or control” (p. 135). The key distinction here is that the information is gathered for a purpose and that that purpose involves some form of action. Data that is simply gathered, but never acted upon or attended to by a human being, does nothing.

Surveillance differs from the more general form, observation, in its more systematic nature. It is practiced by institutions, not individuals. Using the language of cybernetics, I define surveillance in society as the *systematic production of informational feedback about people, processes and institutions which facilitates the internal regulation of a social system*. We can break down this feedback into two branches: 1) the continuous flow of real-time information about the system in question to the regulator and 2) the matrix of stored historical data about this system (memory) accessible to the regulator. While the regulators of many simple cybernetic

systems may operate without this second channel of feedback<sup>3</sup>, social systems and their institutions of surveillance have become very reliant on them.

## SURVEILLANCE IN THEORETICAL CONTEXT

Lyon (2001, p. 109) identifies four, often interwoven, strands in modern surveillance theory: *nation state*, *bureaucracy*, *political economy*, and “*technologic*.” I will describe each of these threads in turn.

### NATION STATE

State institutional actors have a different set of interests than the private sector, although at times these interests merge. In cybernetic terms, the basic function of the state is to act as regulator of the social system, to keep the system within a stable state of homeostasis.<sup>4</sup> Part of that duty is being able to rapidly shift resources to citizens of the state who may most need them and to be able to respond to human threats such as crime, natural disasters, or economic dislocation quickly. In order to perform its job, the regulator must have continuous feedback from the system it is regulating.

Institutions of surveillance are the primary mechanism for providing this feedback function in social systems. The connection between state policing institutions and the reduction of street crime has been traced back to 19<sup>th</sup> century France (Gillis, 1989). Dandaker (1990) and Giddens (1985) describe the importance of surveillance for internal pacification of nation states and in the provision of social services. Gilliom's (2001) ethnography of the welfare bureaucracy

---

<sup>3</sup> A thermostat is the most basic example. Simple life forms, such as amoeba operate on purely real-time sensory feedback as well. Social systems are second order cybernetic systems, a term used in the literature to account for a shift from the cybernetics of observed systems to the "cybernetics of observing (systems)" (Krippendorff, 1996).

<sup>4</sup> According to the Principia Cybernetica, a homeostatic system "is an open system that maintains its structure and functions by means of a multiplicity of dynamic equilibriums rigorously controlled by interdependent regulation mechanisms. Such a system reacts to every change in the environment, or to every random disturbance, through a series of modifications of equal size and opposite direction to those that created the disturbance. The goal of these modifications is to maintain the internal balances." See <http://pespmc1.vub.ac.be/HOMEOSTA.html>.

in Appalachian Ohio provides a detailed picture of the state's interest in knowing intimate details of the lives of its beneficiaries. And Ericson & Haggerty (1997) have shown how tightly interwoven state surveillance institutions have already become with the private sector in the management of risk, describing the role police officers play as knowledge workers for the insurance industry.

The “risk society,” a concept developed by Ulrich Beck (1999), describes a social system oriented around the identification and management of risk. Beck suggests that the risk society emerged as part of an almost evolutionary succession moving from a focus on the importance of institutions in communal and collective structures to an emphasis on individual agency. The risk society is an approach that attempts to mitigate the problems unleashed by modernism itself, such as the increase in crime and sickness that accompanied the growth of densely populated urban areas, or the increase traffic accidents from the proliferation of motor vehicles, or the threat of global warming from industrial pollution. Beck's notion of the risk society can be considered another formulation of the cybernetic definition of surveillance, where regulation of instability becomes the management of risk. For Beck, the increase in risk that world society is experiencing is leading people to rethink the importance of state institutions and governance, but with an emphasis on transnational configuration that can deal with the increase in “de-bordered” risks:

There is a surprising parallel between the reactor catastrophe of Chernobyl, the Asian financial crisis, 9/11 and the consequences of Hurricane Katrina for the American self-image. In each case they led to world-wide discussion of the question, to what extent the dynamic of world risk society must be regarded and evaluated as a historic refutation of the neo-liberal conception of the minimal state. For example, a result of the jolt given by the revelation of the hidden Third World face of the United States has been that, despite the sceptical attitude of many Americans to the state, there has been an opening up of the question as to an appropriate role of government.<sup>5</sup>

---

<sup>5</sup> From a 2006 speech, Hobhouse Memorial Public Lecture, February 15, at the Old Theatre, London School of Economics.

## BUREAUCRACY

Max Weber, the central theorist of this strand, sees surveillance as part of the process of instrumental rationalization, the driving force of the bureaucratic process:

Irrationalities may successfully be eliminated by bureaucratic means, producing rationally calculable administrative action. The surveillance function lies primarily in the files, those dismal dossiers that store information on each individual, the knowledge of which produces and reproduces power. For Weber, bureaucratic surveillance is a means of procuring efficiency, especially in the large scale and unwieldy tasks that confront any expanding modern nation state (Lyon, 2001, p. 110).

By rationalization “Weber meant the process by which explicit, abstract, intellectually calculable rules and procedures are increasingly substituted for sentiment, tradition, and rule of thumb in all spheres of activity” (Wrong, 1970, p. 26). Weber’s work addressed this process of rationalization in economic life, law, administration and religious ethics. As Brubaker (1984) remarks “[i]n each of these institutional spheres, rationalization has involved the depersonalization of social relationships, the refinement of techniques of calculation, the enhancement of the social importance of specialized knowledge, and the extension of technically rational control over both natural and social processes” (p. 2). Weber believed that scientific rationalism “heightens the possibility for political, social, and economic manipulation” (Gandy, 1993, p. 40). More recently, Beniger (1986) interpreted Weber’s rationalization as an instrumental need to reestablish control through efficient management of information. Dossier systems, then, can be conceived as a primary tool of the administrative rationalization of the state.

## POLITICAL ECONOMY

Political economy comprises a number of related approaches, all of which manifest a concern with the way power, as a social resource, becomes unequally distributed and how social inequalities tend to accrue as actors with resources use them to their advantage. The actors may try to influence the law and policy or influence public opinion (Gandy, 1982; Etzioni, 1988).

Political economy challenges the mainstream neo-liberal economic model which largely replaces the concept of power with the invisible hand of the market (Reder, 1999). Information itself is a key resource for the accrual of power.

Robins and Webster (1999) demonstrate how the growth of surveillance practices predated advanced communication and computing technologies, and is instead due in large part to the logic of capitalism. Specifically, surveillance practices began in earnest with “Taylorism,” the emergence of scientific management introduced by F. W. Taylor in the early 20<sup>th</sup> century. Taylorism was a prescription for dramatically improved efficiency of the production process in factories through increased planning and the concentration of skill and information at the managerial level. Information gathering, central to the planning process, led to the increased importance of workplace surveillance, although this was originally managed without the assistance of computers or other advanced communication technologies. As the utility of Scientific Management in the production cycle became clear, its basic principles were extended from the cycle of production to the cycle of consumption, what became known as “Sloanism” after Alfred P. Sloan. As the Taylorist principles of calculation were extended to the marketing sphere, industry started to gather growing amounts of information on individual consumers, on their needs, wants and dispositions, on their demographic and socio-economic backgrounds, leading to the emergence of market research firms. The increasing commodification of information has led to the emergence of the data mining industry in which firms such as Acxiom and Check Point focus exclusively on producing massive databases of personal information that can then be sold to both the public and private sector (Piatetsky-Shapiro, 1999).

Corporations with economic wealth often use their resources to influence government policy in ways that increase the profitability of their business (Etzioni, 1988). Corporations find that investing in policy (often through the lobbying process) they can get a far superior return on

investment than if they make an equivalent investment in improving their product or service. Corporations may also choose to influence debate by providing information to journalists writing about targeted topics, through press releases or more subtle means, such as buzz marketing, and other approaches to manufacturing consent, what Gandy (1982) calls an information subsidy. For many corporations, surveillance and identification systems are good business. The copyright industry has been very vocal about its support for surveillance initiatives. Operating in the other direction, states are driving the growth and transformation of surveillance markets with their own large-scale initiatives, contributing to what the Homeland Security Research Corporation (HSRC) has projected will be a nearly \$300 billion global market by 2018.

#### TECHNOLOGIC

Innovations in communication technologies over the past few decades dramatically increase the scope and reach of possible state surveillance programs. The contribution of technology to surveillance practice is significant enough to warrant a distinction between what Marx (2002) calls traditional surveillance and the “new surveillance.” Gordon Moore, cofounder of Intel, observed in 1965 that the number of transistors per square inch on integrated circuits had doubled approximately every 18 months. This pattern, which persists and is known as Moore’s law, is integrally tied to the fundamental shift in surveillance potential inherent in the emerging electronic social space mediated by computers and the global telecommunication network. As Norris (2003) discusses, the reach and depth of video surveillance has been dramatically expanded with the shift from analog, disparate video tape banks to digitized, networked video surveillance.

The cost of storing data continues to drop dramatically, an average of 40% per year since the late 80s, twice as fast as Moore’s law (Orzech, 2003). The cost to store one terabyte of data was \$1 million in 1992 and around \$127 in 1997. In 2004, Wal-mart alone was storing 460

terabytes of data (Hays, 2004). Internet companies now routinely store customer data even without any extant plan for exploiting the data, on the assumption that it may be valuable to them sometime in the future.

Although technology obviously has played a key role in the character, scope and extent of surveillance in recent human history, scholars must be careful to avoid giving technology too large a role, discounting the critical role of human thought and action. Technology is best thought of as an enabler (or constrainer) of surveillance practice that determines nothing on its own. For example, real time communication between two geographically distinct points was not possible until the invention of the telegraph, but individual, real instances of communication were always the result of human will, of specific human decisions shaped by complex human needs. Gary Marx (2002), who has written extensively about the significance of new technologies in allowing for a quantum increase in the extensiveness of surveillance, is careful to stress that the presence of technological capacity does not mean it will be used. Marx's "surveillance slack" conceptualizes the space between potential and actual surveillance practices:

With sensationalist and often unrepresentative examples, the media talk of the death of privacy with implicit reference to a supposed utopian past and privacy advocates are constantly documenting new risks. In contrast entrepreneurs too often discuss hypothetical benefits of new technologies as if they were fact. In the rhetorical excesses, which shape public awareness, there is a failure to differentiate the potential of a tactic from its actual use. This suggests the need for a broad comparative measure of surveillance slack which considers the extent to which a technology is applied, rather than the absolute amount of surveillance. (p. 23)

Nevertheless, the possibilities introduced by certain recent technological innovations, such as the Radio Frequency Identification (RFID) chip, are significant enough that they create the conditions for possibly discontinuous increases in surveillance practice (Garfinkel, Jules & Pappu, 2005) and dramatically increase the potential reach, scope and depth of state dossier systems.



## POPULAR SURVEILLANCE PROBLEM FRAMES

The various frames for addressing surveillance as a social problem can be a mixture of particular concepts, metaphors and literary references. Frames may be mixed and matched occasionally, so a particular frame becomes an element of a larger argument strategy. Below, I consider a number of common frames and frame elements as well as their weaknesses in facilitating solutions: the word *surveillance* itself, the concept of *privacy*, the metaphor of the *Panopticon*, the term *surveillant assemblage*, and the phrase *data collection*.

### SURVEILLANCE

Though not often conceived of as a frame itself, it does play that function in the general discourse of surveillance studies, for example, when scholars worry about the emerging “surveillance society.” A major problem with the term surveillance as a problem frame is that the actions surveillance affords include vital aspects of modern society.

... there is now some critical debate about the breadth and inclusiveness to the concept of surveillance, which has been expanded to embrace any capture of personal information, whether identifiable or not, and whether having positive or negative implications for the individual. It too, therefore, is a concept that carries a lot of theoretical baggage, and is being in danger of being stretched so far that it, like “privacy,” might mean everything and nothing. (Bennett, 2008, p. 17)

In order to distinguish between the positive and negative aspects of surveillance, further distinctions and additional frame elements are required.

### PRIVACY

The English language concept of “privacy” has been a key rallying point for academics and activists who resist global surveillance regimes. Despite its importance, however, there appears to be a growing chorus of criticisms of the concept’s problematic entailments and

seemingly intractable ambiguity. In his book, *Surveillance Studies: an Overview*, Lyon (2007a) writes:

Conventionally, in the West, privacy has often been seen as the concept around which resistance to intensive or extreme surveillance may be mobilized . . . privacy helpfully alerts us to dimensions of human existence that should rightly be treated with caution and respect, in tandem with principles such as “fair information practices,” offers some vital guidelines as to how surveillance should be regulated. But privacy is also hard to define and varies tremendously from culture to culture and from era to era. It is also associated with possessive individualism, with property and with a dubious notion of persons as autonomous agents. (p. 7)

There is considerable disagreement within American legal and philosophical discourse as to how to define privacy. Posner (1978), for example, notes that the concept of privacy is “elusive and ill defined” (p. 393). Scholars continue to struggle over whether privacy is best thought of as some instrumental term invoked to protect more core values, or if there is something intrinsic in the concept itself that needs to be respected (Fried, 1968; Posner, 1978; DeCew, 1997; Etzioni, 1999). Arguments claiming the intrinsic nature of privacy must tread a fine line. There are other important concepts under the rubric of human rights, such as liberty, security and justice, which privacy cannot simply trump. Baker (2004), for example, argues convincingly that free speech should trump “privacy rights” in many cases (although not for corporate entities). Allen (2003) has made a convincing case that privacy can conflict with accountability in ways that may raise the likelihood of certain social injustices. Etzioni (1999) has shown how strong privacy rights for individuals could have dramatically negative effects on public health. Several government officials and academics make the case that privacy can compromise security and thus should have even less sway in the 21<sup>st</sup> century than it did in the simpler past (Posner, 2006; Singel, 2007a). Many argue that the privacy value always puts individual over group interests. As Rule (2007) notes, “[d]esires for privacy often map efforts to assert one’s own interests or individuality in the face of countervailing claims” (p. 10).

## THE PANOPTICON

Perhaps the most common metaphor used when problematizing surveillance in social systems is the “Panopticon.” Foucault (1979) uses the architectural design of a prison, conceived by Jeremy Bentham, as a diagram of modern systems of power, discipline and punishment. The Panopticon is composed of a central tower surrounded by a number of isolated cells arranged around the tower in a circular pattern. The cells have two windows, one opening to the outside, to allow light to come in and illuminate the occupant, and the second facing the central observation tower. Each cell is walled off from the others, while the lighting and design of the central tower makes it impossible for cell occupants to see the guards that may or may not be watching them. This arrangement leads to a dramatic imbalance in the flow of information between watcher and watched:

The Panopticon is a machine for disassociating the see/being seen dyad: in the periphic ring, one is totally seen, without ever seeing; in the central tower, one sees everything without ever being seen. (pp. 210-2)

The result, Foucault writes, is a power play, the habitual inducement of discipline and institutional normality in the subjects of surveillance:

Hence the major effect of the Panopticon: to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power. So to arrange things that the surveillance is permanent in its effects, even if it is discontinuous in its action; that the perfection of power should tend to render its actual exercise unnecessary; that this architectural apparatus should be a machine for creating and sustaining a power relation independent of the person who exercises it; in short, that the inmates should be caught up in a power situation of which they are themselves the bearers. (p. 201)

Although the oft-used panoptic metaphor suggests perfect centralization, academic treatments of surveillance over the past two decades rarely attempt to suggest that such integrated totalizing surveillance is the reality of the world today. Instead, there is an expectation that many key mechanism of surveillance remain largely separate from one another. For example, Ball &

Webster (2003) note important questions regarding just how centralized systems of surveillance have become:

It might be noted that recent Foucaultian accounts of the panopticon tend to resist the suggestion that panoptic techniques have become homogenized and centralized ...in the hands of say, linked transactional corporations or integrated government agencies.... Gandy (1998), for instance, asserts that it would be a mistake to assume that surveillance in practice is as complete and totalizing as the panoptic ideal type would have us believe. For instance, it may be that educational institutions and retail corporations operate as huge panoptic machines in themselves, but these are both internally differentiated and externally hard to access by others, while the surveillers within education and the retail industry are themselves surveilled by many other panoptic-like organizations such as insurance companies and tax agencies. In this sense, today's surveillance may more accurately be seen as at once more pervasive and less centralized than might have been imagined by earlier proponents of panopticism. (Ball & Webster 2003, p. 6)

#### THE SURVEILLANT ASSEMBLAGE

Other scholars, such as Haggerty & Ericson (2000) have argued that surveillance systems are far more interconnected than Ball & Webster suggest, although they replace Foucault's centralized panoptic architecture with Deleuze and Guattari's metaphor of the *rhizome*.<sup>6</sup>

... we are witnessing a convergence of what were once discrete surveillance systems to the point that we can now speak of an emerging 'surveillant assemblage'. This assemblage operates by abstracting human bodies from their territorial settings and separating them into a series of discrete flows. These flows are then reassembled into distinct 'data doubles' which can be scrutinized and targeted for intervention. In the process, we are witnessing a rhizomatic leveling of the hierarchy of surveillance, such that groups which were previously exempt from routine surveillance are now increasingly being monitored. (p. 606)

To speak of the surveillant assemblage risks fostering the impression that we are concerned with a stable entity with its own fixed boundaries. In contrast, to the extent that the surveillant assemblage exists, it does so as a potentiality, one that resides at the intersections of various media that can be connected for diverse purposes. Such linkages can themselves be differentiated according to the degree to which they are ad hoc or institutionalized. By accentuating the emergent and unstable characteristic of the surveillant assemblage we also draw attention to the limitations of traditional political strategies that seek to confront the quantitative increase in surveillance. As it is multiple, unstable and lacks discernible boundaries or responsible governmental departments, the surveillant assemblage cannot be dismantled by prohibiting a particularly unpalatable

---

<sup>6</sup> A rhizome is a biological term, referring to a kind of horizontal stem that sports a large number of shoots and roots growing from its multiple nodes. The term was first used in critical theory by Deleuze and Guattari and was adopted by Haggerty & Ericson (2000) in their "surveillant assemblage" concept.

technology. Nor can it be attacked by focusing criticism on a single bureaucracy or institution. In the face of multiple connections across myriad technologies and practices, struggles against particular manifestations of surveillance, as important as they might be, are akin to efforts to keep the ocean's tide back with a broom — a frantic focus on a particular unpalatable technology or practice while the general tide of surveillance washes over us all. (p. 609)

Although they are right to point out the inadequacy of the panoptic metaphor, Haggerty & Ericson (2000, *above*) fail to consider the potential applicability of Foucault's broader work in discourse theory to help consider the "structuring structures" of surveillance. Although they suggest that their "surveillant assemblage" helps elucidate the futility in adopting surveillance policies technology-by-technology or issue-by-issue, they fail to make clear how the concept of an assemblage provides a more useful purchase for public interest policy. There is certain inevitability in their talk of surveillance that is very common in the literature today. The plus side, they seem to think, is that the gaze will be on people throughout the hierarchy and not just some lower class:

New media, particularly television, allow the general public to scrutinize their leaders as never before (Meyrowitz 1985). We need only consider the media circus which surrounds Britain's royal family to acknowledge this point. Furthermore, the monitoring of the powerful has been eased by the proliferation of relatively inexpensive video cameras. These allow the general public to tape instances of police brutality, and have given rise to inner-city citizen response teams which monitor police radios and arrive at the scene camera-in-hand to record police behaviour....While not a complete democratic leveling of the hierarchy of surveillance, these developments cumulatively highlight a fractured rhizomatic crisscrossing of the gaze such that no major population groups stand irrefutably above or outside of the surveillant assemblage. (p. 618)

While it is certainly true that the ubiquity of camera-equipped cell phones and other ICTs have made police and other government agents more susceptible to citizen surveillance, it would be a mistake to assume that there has been even a partial leveling of the surveillance hierarchy vis a vis the state. Further, while it the "surveillant assemblage" may provide an accurate model for how surveillance activities takes place in real time, surveillance data in stored form flows most significantly in one direction, toward state database systems.

## DATA COLLECTION

In her examination of the role of language and metaphor in science, Anne Salmond (1982) argues that, in the West, knowledge is nearly always conceived as a landscape, while facts are objects to be found within this landscape:

Facts are depicted as hard, solid, concrete and tangible — they are to be picked up, collected, gathered, dug up, sorted, sifted, weighed, balanced, arranged and looked at....

Facts are objects, described in group nouns, with a physical existence and of natural origin....A fact may be mineral, to be mined and excavated, or vegetable, to be gathered and preserved, cultivated and even cooked (from raw facts to half-baked theories). This is the true metaphorical basis of “objectivity”, presupposed in our everyday talk about what is. It is also the linguistic rationale for the persistent idea that field-work is data gathering, as though the important features of another society will be lying about on the ground for our collection (p. 75)

Major privacy advocates today regularly define problems related to surveillance and privacy in terms of personal information collection. In his book, the *Digital Person*, one of the most important works today warning of the dangers of the emerging dossier society, Solove (2004) writes “[j]ust as the Food and Drug Administration (FDA) regulates food and drugs . . . we need a federal agency to regulate the collection and use of personal information” (p.108). David Lyon defines surveillance as “any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered” (2001:2). Gary Marx (2005) writes that the contemporary commercial state is “inconceivable without the massive collection of personal data” (n.p.).

When we speak of “collecting” or “gathering” personal information, we are participating in the long, linguistic tradition of treating information and facts as natural objects existing out there in the landscape. In many contexts, particularly in those circumstances where real-time surveillance, or third-party aggregation and analysis (data mining) is a concern, this particular metaphoric approach works quite well. As with any metaphor, however, the approach highlights

certain aspects of the problem while hiding others. The terms “collection” and “capture” include a built-in assumption that the information gathered already exists “out there” before it is collected. Although collection is an active term, it is passive in relation to the data itself. Focusing on collection ignores the very critical processes that lead to the creation and storage of personal information in the first place, processes which need to be much better understood if policy is to have any chance at regulating the emergence of dossier systems worldwide. The problem society faces is not simply about the collection and aggregation of data, but of modes of practice that produce particular kinds of personally identifying information, information that then leads to a particular way of seeing state subjects that may not always be in the public interest.

The weakness of a particular frame or frame element can be due to a number of different factors. It might be that the term itself is too abstract or difficult to define, or it may be too strongly associated with individual over collective interests (*privacy*); its entailments might seem a poor fit for the problem in its current configuration or overestimate the powers of certain relevant institutions (*panopticon*); it may be so general and all encompassing as to include both critical social functions and problematic behavior (*surveillance*); it may define an emergent phenomena in a way that it appears to be a *fait accompli* for which nothing can be done (*surveillant assemblage*); or it may suggest a passive relationship to personal data that hides the logic of its production (*data collection*). Clearly, no frame is perfect. And just because a frame has a particular weakness does not render it useless for analysis or political advocacy. Nevertheless, it seems clear that the relatively young field of surveillance studies would benefit from some alternate frames.

The primary goal of this dissertation is to introduce, explore and demonstrate the utility of one such alternate frame: the *emergence and continued development of state dossier systems*, massive databases of comprehensive personal information linked to national identification

systems. In this problematization of the state dossier system, the dissertation seeks to answer the following core research questions: what are the major components of dossier systems and what are the forces that propel and hinder their construction?

## PLAN OF DISSERTATION

### CHAPTER 2, PROBLEMATIZING THE STATE DOSSIER SYSTEM

This chapter introduces the “state dossier system” as a problem frame. It is divided into four major sections: *Origins of State Dossier Problematization* examines the origins of this frame from a literature and historical perspective; *Conceptual Elaboration* introduces the frame’s key concepts, uses them to expound upon the core problem, and introduces the primary research questions; *The Problem* defines the general model of the state dossier system, examines its three key dangers, identifies the core research questions and presents four driver's of dossier systems drawn from surveillance studies scholarship; finally, *Method* describes the method of data gathering and analysis that drove the dissertation research process.

### CHAPTER 3, U.S. HISTORICAL CONTEXT

This chapter provides a brief historical and legal context for understanding the current configuration of the U.S. dossier system. As a largely heuristic device, and to simplify a very complex tapestry of law and policy that has impacted the evolution and configuration of the U.S. dossier system over the past several decades, I break down the U.S.’s “dossier history” into three phases. In the first phase, from the mid 1920s to the mid 1979s, the U.S. exhibits all the characteristics of a full-fledged state dossier system. In the second phase, from the mid 1970s until 2001, federal laws and policies are in place to put “walls” blocking information flow between government agencies. In the third phase, beginning in the fall of 2001, the “walls” policy is reversed and replaced with new government thinking that “connecting the dots” and information sharing between and across government agencies should be paramount.

### CHAPTER 4, U.S. CASE

This chapter examines the current state of the U.S. dossier systems in terms of the two primary components of the general model: *ID systems* and *systems of records*. The ID systems section first provides a brief historical overview of state driver’s licenses and the social security system before analyzing the federal government’s case and the public’s reaction to a set of national standards for state-issued driver’s licenses, the Real ID initiative. The systems of records section, divided into three sub-sections, considers U.S. record systems at two levels of analysis: 1) record systems as wholes and 2) types of records.



## CHAPTER 5, PRIVACY ACROSS CULTURES

This chapter has two primary goals: 1) to establish common ground for the problematization of state dossier systems connecting two highly distinct case studies on the basis of information privacy and 2) to advance the academic discourse concerning the role and meaning of privacy within the global context of surveillance studies.

## CHAPTER 6, CHINA CASE

This chapter describes China's state dossier system as it existed in the 1980s and explores four primary sites of production — government departments, schools, work places, and local public security bureaus — each with their own slightly different but ultimately harmonious logics. Next, it describes three major transitional forces that have helped to revolutionize the production of the dossier: 1) labor mobility, 2) globalization and 3) ICT modernization. After reviewing these transitional forces, it looks more specifically at the current state of the two primary dossier system components, ID systems and systems of records. Finally, the conclusion summarizes the problem of the state dossier system in China today - in particular, its unfinished, contingent nature.

## CHAPTER 7, SYNTHESIS

The two case studies were chosen for two primary reasons: 1) to provide some independent gauge for the intensity of the current U.S. dossier problem and 2) to help drive the development of general terms for the problematization of state dossier systems. That the U.S. and China come from two entirely different political traditions is indisputable, but the practical differences today, when it comes to the ongoing evolution of state dossier systems and the specific constraints they encounter, are not as significant as we might assume. This chapter juxtaposes the two cases more directly to make this point. The chapter revisits the four drivers of dossier systems outlined in chapter 2 and explores in more detail the linguistic toolkit that has been developed for state dossier system analysis, including terms like the “sites” and “logics of production and the “targeted person.” Next, the chapter reviews some of the more potentially controversial propositions that have been presented here and the evidence on which they are based, and offers some concluding thoughts.

## CHAPTER 2: PROBLEMATIZING THE STATE DOSSIER SYSTEM

The primary goal of this chapter is to introduce the “state dossier system” as a problem frame. It is divided into four major sections: *Origins of State Dossier Problematization* examines the origins of this frame from a literature and historical perspective; *Conceptual Elaboration* introduces the frame’s key concepts; *The Problem* defines the general model of the state dossier system, examines its three key dangers, identifies the core research questions and presents four driver’s of dossier systems drawn from surveillance studies scholarship; finally, *Method* describes the method of data gathering and analysis that drove the dissertation research process.

### ORIGINS OF STATE DOSSIER PROBLEMATIZATION

The whole dossier continues to circulate, as the regular official routine demands, passing on to the highest Courts, being referred to the lower ones again, and then swinging backwards and forwards with greater or smaller oscillations, longer or shorter delays....No document is ever lost, the Court never forgets anything. One day - quite unexpectedly - some judge will take up the documents and look at them attentively.... “And the case begins all over again?” asked K. almost incredulously. “Certainly” said the painter. (Kafka, *The Trial*, 1925, cited in Solove, 2004, pp. 36-37)

Franz Kafka’s *The Trial* tells the story of Joseph K., a citizen of what he has always thought was a free country, who suddenly finds himself accused of a crime. Joseph K. is forbidden from knowing his crime or seeing the evidence the state has amassed against him. The unseen documents that comprise Joseph K.’s dossier remain in circulation and may be used by the state as evidence against him at any time in the future. In the story, that future eventually arrives and Joseph K. is seized from his house and summarily executed.

Legal scholar and privacy expert Daniel Solove (2004) has argued that the metaphor of Kafka’s *The Trial* should be invoked to complement the much more common uses of Foucault’s *Panopticon* and George Orwell’s *1984* in academic and popular writing about surveillance as a

social problem. *The Trial* communicates, through exaggeration, the helplessness individuals can feel in the face of these massive personal data stores that they can never really see but have so much power over their lives. I find *The Trial* metaphor particularly compelling because of its focus on the danger of the stored data that persists. The ultimate force that is haunting Joseph K. is not some powerful state institution watching his every move 24 hours a day. Rather, it is an immense mass of stored data about him that will persist and shadow him throughout the course of his life. While the *Panopticon* emphasizes the real-time watchful eye of the state, Kafka's story focuses on the practically eternal mass of symbolic stored data — personal information that may easily outlast a particular state or regime, and which can serve as the raw material for the construction of new crimes and the development of new punishments.

As we see in *The Trial* story, the dossier is a file of tremendous social force that can contain personal information that is highly broad in scope and deep in detail. The dossier is actively compiled by agents of the state and thus is always changing. The dossier is perpetually incomplete and error ridden, but also full of information among the noise. The state dossier system frame, which I will introduce in detail below, is focused on the three-way relationship between the state, the dossier, and the people.

Although the term will be discussed more fully in the paragraphs that follow, it is helpful to first begin with a simple definition of “state dossier system.” In short, a dossier system is composed of two key subsystems: 1) personal identification and 2) a system of records containing personal information. A dossier system contains a range of information types regarding dossier subjects, both in semantic content and quality, from raw data listing websites visited in a given day to polished, psychological profiles prepared by trained professionals, such that the combined data paints a relatively “complete” picture of the data subject.

Below, I will consider the state dossier system's historical association with government oppression, and then consider some of the major entailments, key concepts of the frame that need to be defined before a more detailed elaboration on the categorization of state dossiers as a social problem can be made. Once I have reviewed the chief concerns of this frame and how it can be distinguished from other frames, I will return to and expand upon the definition of state dossier system and the relationship between its primary components: identification technology and personal record systems.

### DOSSIERS IN HISTORY

If one looks at recent history, one can see in several nation states, including Nazi Germany, Soviet Russia, Communist China, South Africa, East Germany and Rwanda, a strong association between the key components of the state dossier system and government oppression. In the worst, most well known cases of oppression, including Nazi Germany, Soviet Russia, and modern China in the late 60s through early 80s, both components of the system were in active use and worked in concert. The Soviet Union and modern China developed particularly detailed personal record systems that reflected a total (totalitarian<sup>7</sup>) interest the citizen subject, an interest that went beyond keeping them inline and obedient to include their active spiritual and cultural cultivation.

... the collection of information was not an end in itself: surveillance was not primarily intended to reflect public opinion, nor was it meant merely for the preventive, protective task of forestalling any possible opposition (although it was most certainly put to that use, too). Surveillance was an instrumental endeavor, aimed at reshaping society and transforming every individual in it. And it was only as part of this larger project of transforming each and every individual that surveillance was used to recognize the recalcitrant (so they could be singled out for special attention) and, later, to identify those impervious to improvement (so they could be eliminated and no longer pollute the body politic....This is not a minor or semantic distinction. Soviet citizens knew surveillance was instrumental. They knew (though how extensively most could not guess) that, through surveillance, the state was not only reporting what they said and wrote but also

---

<sup>7</sup> This term will be addressed in detail below.

seeking to use this information to change and correct them and their views. Surveillance was not a passive, observational endeavor; it was an active, constructivist one. (Holquist, 1997, p. 417)

At times, such as in the case of Nazi Germany, South Africa and in earlier Soviet history under the Cheka secret police, the state's interest in gathering information was primarily to identify and constrain or eliminate "enemies of the state," a term that could be very widely construed.

Information is the alpha and omega of our work.

Our work should concentrate on the information apparatus, for only when the Cheka is sufficiently informed and has precise data elucidating organizations and their individual members will it be able ... to take timely and necessary measures for liquidating groups as well as the individual who is harmful and dangerous. (Cheka circulars, 1920-21, quoted in Holquist, 1997, p.

In Nazi Germany, the Third Reich made use of a complex data system of punch cards maintained by International Business Machines (IBM), a system which was instrumental in the roundup and eventual extermination of millions of Jews:

Jews could not hide from millions of punch card thudding through Hollerith machines, comparing names across generations, address changes across regions, family trees and personal data across unending registries...Even as Hitler's fanatic followers thundermarched through Nuremberg, Hollerith machines in Berlin were dispassionately clicking and rattling through stacks of punch cards slapping into hoppers to identify the enemy for the next drastic measures. (Black, 2001, p. 105, quoted in Sobel, 2002)

In South Africa, the white minority government's practice of apartheid was greatly facilitated by a computerized passbook system made possible by a number of U.S. IT corporations including IBM and Burroughs:

More than any other single technological advancement, the computer has fostered the concentration of administrative power in the hands of South Africa's white elite. Since the days of the first automated population register, computer use has spread to virtually every government department, playing a key role in Pretoria's ability to manage the African, Asian and Indian population. ("Automating Apartheid," 1982, p. 14)

Historians largely agree that the Rwandan genocide in 1994, in which more than 500,000 ethnic Tutsis and politically moderate Hutus were killed, was greatly facilitated by the presence of national ID cards with ethnic group classification introduced by the Belgian colonial government in 1933 (Longman, 2001). The ID card system, in addition to facilitating the identification of genocide targets, served to psychologically distance the killers from the civilians they were instructed to kill. This type of distancing, argues Fussell (2004), occurs “whether the task is genocide, deportation or applying discriminatory restrictions” (p. 65).

Soldiers had orders to take identity cards from those whom they killed. According to one witness, Nizeyimana regularly received these cards from his men as they reported on the progress of the killings. They often appeared at his house shortly after a volley of gunfire was heard and handed the cards to the captain with the report, “Mission accomplished.” In the captain’s absence, his wife received the cards. (p. 65)

The Rwandan genocide appears to be connected mostly to an identity card and the ethnic classification it bore, rather than any detailed system of personal records. It is important to recognize that the decision to place the identity on the card, indeed the decision to make the ethnic distinction in the first place, merely afforded the genocide. It still took a failure of humanity for the act that followed. Once in place, however, dossier systems may be appropriated by states with different intentions.

Although a detailed “population registry” system had been part of the Dutch bureaucracy since the early 1800s, the program was not an instrument of government oppression until it was put to different use by the occupying Nazi army during WWII. The Dutch “personal card system” contained information about each citizen’s religion, occupation, disabilities, and other characteristics. Writing in the General Archive of Statistics, about the modern population registry in 1936, overseeing statisticians Methorst and Lentz wrote “[t]heoretically, the collection of data for each person can be so abundant, and even complete, that we can speak at last of a paper human who represents the natural human” (Aly et al, 2004, p. 66). In the state’s comprehensive

population registration system, all civil rights, duties, and benefits of citizenship were based on registration. The Dutch registry provided the invading Nazi army with detailed lists of Jews and their locations that were unavailable to them in other European countries like France, and was further developed into a highly sophisticated ID card system which made it particularly difficult for Jews to go underground or find black market jobs (Moore, 1997).

As we explore this term in detail, we will see that state dossier systems are in many ways relatively new phenomena, as they are dependent on modern electronic networked communication technology to achieve their scope and depth of coverage. Nevertheless, states in history have implemented national ID card systems and comprehensive file systems on their citizens, and these practices have been associated with government oppression so extreme that it led to the emergence of a new term: *totalitarianism*.

Historically, when states begin to keep comprehensive detailed files on their citizens, injustice has often followed. Can we conclude that state dossier systems are in essence totalitarian? Solove, points out that Kafka's story of *The Trial* shows us a world in which the personal file can end up terrorizing us without any larger, socially disruptive program organized and directed by the state. In Kafka's world, there was no active state program to spiritually mold and educate its citizen or to terrorize and eliminate the "opposition," only a simple reverence for files, documents and bureaucratic procedure.

In order to examine the concept of the state dossier system in more detail, we need to consider its key entailments and core concepts, including the concept of totalitarianism, its definition, and its present utility in illuminating potentially dangerous scenarios of our global future that political leaders, social activists and academics must work together to prevent.

## CONCEPTUAL ELABORATION

To better understand the entailments of the state dossier system frame, I will introduce a set of key concepts to which I refer when considering the problem. These concepts vary in their level of abstraction, in the formality or informality of their definitions, and in their diffusion into the lexicon of broader academia and public discourse, but they play an important role in helping to illuminate the space of relations (actual and possible) that constitute a state dossier system: *privacy*, *totalitarianism*, *identity*, *system of records*, *personally identifying information*, *production*, *data shadow/ data double*, and *affordance*. These are not in all cases “components” of the state dossier system, but concepts of distinction which help us to both problematize and make sense of it. Although it would be possible to present these terms in a continuous logical narrative, it would be artificial and eventually constricting to their utility in analysis. Instead, I present each concept on its own terms, under its particular heading. Once I have discussed these key concepts, I will then elaborate more specifically how the state dossier system should be seen as a significant social problem.

### PRIVACY

As was discussed in chapter 1, there is considerable disagreement within American academic discourse as to how to define privacy. For the purposes of this dissertation, I wish to focus on the work of two privacy scholars which have particular relevance to the study of state dossier systems, Altman’s (1981) work on privacy as an “interpersonal boundary process” and Nissenbaum’s (2004) theory of “contextual integrity.”

### INTERPERSONAL BOUNDARY PROCESS

Social psychologist Irwin Altman (1981) presents a comprehensive, but highly abstract model of privacy as an “interpersonal-boundary process.” Individuals and groups negotiate a



dialectic tension between a need for openness and “closedness” to the outside world, as conditions and circumstances change:

... privacy is not solely a “keep-out” or “let-in” process; it involves a synthesis of being in contact with others and being out of contact with others. The desire for social interaction or non-interaction changes over time and with different circumstances. The idea of privacy as a dialectic process, therefore, means that there is a balancing of opposing forces—to be open and accessible to others and to be shut off or closed to others—and that the net strength of these competing forces changes over time. (p. 23)

Altman’s boundary negotiation model consists of eight distinct “privacy situations” accounting for management of both inputs and outputs and the difference between desired and achieved privacy. Cases 1-4 deal with the control of input from others, while cases 5-8 deal with the control of output to others. Half of all cases involve situations in which individuals managing their interpersonal boundaries have achieved a desired level of privacy while half represent some type of imbalance, either too little privacy or too much privacy.

Key to Altman’s boundary negotiation theory are the resources — what he calls “privacy mechanisms” — individuals and groups have available to them in the management of boundaries. Altman makes four primary distinctions here: 1) verbal, 2) non-verbal, 3) environmental, and 4) culturally-based privacy mechanisms. Verbal mechanisms would include specific requests to be left alone or, when a couple or small group desires privacy from surrounding “others,” the use of a foreign language. Non-verbal mechanisms include various forms of body language and facial expressions. “Gaze aversion,” for example, can be a signal to others that one is not interested in interaction, and thus can be used for limiting contact. Environmental mechanisms include the use of clothing and adornment, the management of personal space, and finally, the use of more general environmental features such as territories, areas and objects. Finally, culturally-based privacy mechanisms refer to the distinct norms and customs of particular societies and cultures.

Going forward, I am less concerned with Altman's attempt to categorize privacy mechanisms than his more general abstract notion that privacy is a dialectic negotiation afforded by resources. Instead of using his term "privacy mechanism," however, I will use the term "boundary resource." As we shall see, numerous subcategories of these "boundary resources" may be identified, including legal, technological, normative and linguistic resources. By leaving the categorization scheme open and recursive, however, we can avoid blind spots that might emerge from too strict a taxonomy, while facilitating research across cultural and discursive systems. Boundary resources are key to the negotiation of privacy within any social system. Their distribution is dependent on state policies, law and individual cultural and technological innovations, but they may transfer effectively between even highly dissimilar nation states such as China and the U.S..

Altman's theory of privacy as boundary negotiation has been highly influential within the social sciences (Margulis, 2003). The dialectic approach to privacy appears to avoid some of the pitfalls of arguing over instrumentality vs. basic right. Rather than attempt to define privacy in more explicit or static terms, we can focus our attention on the distribution and availability of boundary resources. A focus on boundary resources (legal, normative, technological, linguistic) may also allow policy makers and cultural innovators opportunities to make incremental changes to the privacy environment without whole cloth reconfiguration of communication practices that broader reconceptualizations might entail.

The theory's high level of abstraction and focus on the role of one's physical environment rather than mediated communication, however, has made it difficult to apply to 21<sup>st</sup> century situations without further conceptual development. Scholars have offered a wide range of classificatory schema for boundaries in the hopes of adding empirical analytical power (Derlega & Chaikin, 1977; Petronio, 2002; Palen & Dourish, 2003), but they have yet to converge, in part

because of the complex and dynamic nature of the privacy concept itself. Rather than follow this path, I wish to narrow Altman's general definition of privacy to more specific circumstances of "information privacy." With this added semantic constraint, I consider openness and closedness to the outside world in terms of the creation and flow of personal information, a phenomenon that can be observed in all cultures of the world.

#### CONTEXTUAL INTEGRITY

Rather than attempt to develop a comprehensive theory of privacy, Nissenbaum (2004) carves out a narrower goal of developing a "theoretical account of a right to privacy as it applies to information about people."<sup>8</sup> Nissenbaum notes that public deliberations over privacy are usually based on three prevailing principles: 1) protecting the privacy of individuals against intrusive government agents, 2) restricting access to intimate, sensitive, or confidential information, and 3) curtailing intrusions into spaces or spheres deemed private or personal. Although these principles have been effective in protecting privacy in traditional scenarios such as a policeman seeking to gain entry into your home or someone gaining unauthorized access to the case notes of your psychologist, these principles apply less well to what Nissenbaum describes as technologically mediated instances of "public surveillance." Such cases include the availability of public records online and consumer profiling and data mining. To deal with these new scenarios, Nissenbaum offers the concept of contextual integrity.

In short, contextual integrity is a principle which is designed to limit access to and distribution of personally identifiable information that on its own may not be considered sensitive and may not require intrusions into private spaces by government or private agents to acquire. It is designed to protect your privacy in information that may be stored on databases far from your place of residence.

---

<sup>8</sup> This is often referred to in the literature as "informational privacy."

Contextual integrity is based on two informational norms: appropriateness and distribution. Norms of appropriateness “dictate what information about a person is appropriate, or fitting, to reveal in a particular context” (p. 120). It may be appropriate, for example, to reveal information about your sexual habits to your doctor, or your salary to your banker, but not vice versa. Further, it might be appropriate for your doctor to reveal information about your latest medical procedure to your insurance company, but not your employer. Distribution deals with the “movement or transfer of information from one party to another or others” (p. 122). Norms of distribution focus not on whether the information is appropriate for a given context but whether its flow respects contextual norms of information flow. If Amazon stores the purchase and book browsing patterns of its customers so that it may offer suggestions of new books of interest and does not sell this information to third parties, it is not in violation of the norm of distribution. Contextual integrity is violated if one or both of the two norms is violated.

Nissenbaum’s theory of contextual integrity provides a powerful conceptual tool for analyzing the potential impact of emerging state dossier systems:

According to the theory of contextual integrity, it is crucial to know the context - who is gathering the information, who is analyzing it, who is disseminating it and to whom, the nature of the information, the relationships among the various parties, and even larger institutional and social circumstances. It matters that the context is, say, a grocery store as opposed to, say, a job interview or a gun shop. When we evaluate sharing information with third party users of data, it is important to know something about those parties, such as their social roles, their capacity to affect the lives of data subjects, and their intentions with regard to subjects. It is important to ask whether the information practice under consideration harms subjects; interferes with their self determination; or amplifies undesirable inequalities in status, power, and wealth. (p. 137)

#### PRIVACY VS. INFORMATION PRIVACY

With the new reality of ubiquitous network communication technology, the emphasis of privacy concerns appears to be squarely upon information privacy. Yet how do we distinguish between privacy and information privacy? Are they distinct or is one reducible to the other? This

is ultimately a philosophical question that I do not intend to solve in this dissertation, but it is also a practical one. Allen (1996) advises theorists to tread carefully:

Is physical privacy reducible to informational privacy? The Fourth Amendment restricts access to people, households and other private areas, while also restricting access to information of the sort that might be contained in a person's papers, effects, and conversations. Since physical contact can yield new information, one might take the view that concerns about restricting physical access ultimately boil down to concerns about information learned through sensory exposure. . . .

From the point of view of the person whose privacy is at issue, uncovering information about a person and uncovering the person can be invasions of different dimensions. For example, although both invasions are offensive, it is probably less assaultive to have one's sexual orientation revealed as a result of unauthorized access to one's bedroom during a sex act (a physical invasion). (p. 148)

I believe it is fair to say that privacy has much broader connotations that are lost under the rubric of information privacy, but what we lose in richness we may gain in analytical clarity. I offer a working definition of information privacy (which can in many cases stand in for the more elusive "privacy") in the following way: a state of successfully shielding the observation or creation of any piece of extant data (a record, a sentence, an image, a sound recording) that is linked to a unique individual; a negotiation to reach this state that is afforded by boundary resources (Altman's privacy mechanisms).

By focusing on the term information privacy, I do not want to dismiss more direct, physical aspects of its parent concept. Nevertheless, information privacy can be understood to apply to a wide range of situations in which the common denominator is personal information, regardless of its form or medium. Further, information privacy is resonant with Altman's dialectic negotiation model. As individuals, we expect to exercise some control over the extant information that is associated with us, for example, by choosing when to speak and when to hold our tongues, when to write a letter to the editor and when to make a notation in our locked diary, or when to simply forget. To lose control over this process is to lose control over the construction of our own identities (Gavison, 1980; Cohen, 2003).

Information privacy is about information that is associated with individual people. How we determine this, how we classify a piece of information as being “personally identifiable” turns out to be a highly complex question with no simple answer. Whether a particular piece of information is personally identifiable depends a great deal on the resources of the observing party, not to mention the specific content and context of a message. How the information is created and how it is associated with its subjects is a key question in need of more research. Technologies of identification, which afford the production of personally identifiable information (PII), are developing at a rapid pace.

#### TOTALITARIANISM

... the control and monopolisation of information permitting the surveillance of a population, with the disappearance of the more disaggregated class-divided societies, is a potent medium of power. ‘Classical social theory’ did not recognise the potentiality of what has become in our day a fundamental threat to human liberties, totalitarian political control maintained through a society-wide system of surveillance, linked to the ‘policing’ of day-to-day life. The expansion of surveillance in the hands of the state can support a class-based totalitarianism of the right (fascism); but it can also produce a strongly developed totalitarianism of the left (Stalinism). (Giddens, 1985, pp. 174-5)

The concept of totalitarianism, most famously promulgated by Hannah Arendt (1951), has been subject to considerable debate and criticism within academia. Outside of a general agreement that Nazi Germany and Stalinist Russia exhibited historically unprecedented control over the lives of their citizens, many have criticized Arendt’s conceptualization as essentially too brittle to be useful as a tool for general political theory. I will not attempt to provide a definitive definition of the term here, but explore some of the most common associated characteristics and their relevance for the problem of state dossier systems today.

What distinguishes a totalitarian government from a merely tyrannical or despotic government is the degree to which the totalitarian government “penetrates every pore of the social organism” (Tucker, 1965, p. 560). This penetration of the mass public dramatically reduces the

potential for violent resistance that simmers under the surface of any tyrannical state. The public is shaped and molded according to a unitary state ideology, while at the same time being stripped of any potential for spontaneous human associations. “Individual spontaneity-in thinking, in any aspiration, or in any creative undertaking-that sustains and renews the human world is obliterated in totalitarianism. Totalitarianism destroys everything that politics, even the circumscribed political realm of a tyranny, makes possible” (Kohn, n.d., n.p.).

For Arendt, a key aspect of the totalitarian state, the chief means through which it reduced humanity’s capacity for creativity, innovation or any form of resistance to the state’s agenda, was the widespread, indiscriminate visitation of terror upon the mass public. Highly sophisticated population registries linked to internal passports or national identity cards were an instrumental part of this process in the prototypical totalitarian regimes of Nazi Germany and Stalinist Russia.

While the visitation of violence and terror upon the mass public was a critical component of Arendt’s conceptualization of totalitarianism, other scholars have suggested a different scenario. Kassof (1964) conceived a form of totalitarianism in which such active violence is not necessary, where the penetration of the mass public is achieved via highly efficient forms of bureaucracy and administration.

Convinced that there should be complete order and predictability in human affairs, the elite is concerned not merely with the “commanding heights,” but also to an overwhelming degree with the detailed regulation of the entire range of social life, including those institutions which, in the West, typically have been regarded as lying beyond the legitimate scope of public authority and political intervention. The rulers of the administered society refuse to grant the possibility of unguided coordination and integration; they believe, on the contrary, that not only the masses but responsible subgroups (for example, the professions) are incapable of maintaining viable social order on their own, without the precise and detailed supervision of an omniscient political directorate. (p. 559)

Similarly, Los (2006) suggests that different forms of terror can be visited upon the public without the widespread mass violence of the prototypical totalitarian regimes. Instead, the regime atomizes the mass public via the radical destruction of trust:

... totalitarian surveillance aims at a radical destruction of trust. Its key mechanism involves a conversion of every member of society into a police surrogate for both oneself and others. The penetration of society by the secret police and its collaborators induces pervasive fear, suspiciousness and mistrust. Consequently, each individual not only views all others as potential spies but must also be aware of being similarly viewed by others. This creates painful barriers of fear and humiliation that divide and terrorize society. People have no way of verifying who is a secret agent and have no way of preventing others from suspecting them of being one. The resultant culture of fear and suspicion atomizes society and thwarts social resistance. (p. 83)

For the extant literature on totalitarianism to be of relevance to the current study of dossier systems, it is not necessary to define the term definitively or engage in all or nothing propositions about whether this or that state government is or will be “totalitarian” but rather “to a study of how states might (or might not) employ certain practices in a totalitarian manner” (Holquist, 1997, p. 450). Although it may be tempting to think we have learned from history, and current safeguards in the law and practical political wisdom will keep living, real-world social systems far from the “basin of attraction” that is the totalitarian project, avoiding this eventuality will take continued vigilance and a deep understanding of the factors that could both propel and inhibit the emergence of a “dossier society” centered around extremely powerful state institutions.

## IDENTITY

Identity is such an important, salient topic for humanity as a whole that it can be very difficult to talk about it without raising controversy. Identity is about who we are as individuals and as groups. A key distinction we need to bear in mind right up front is that between identity and identification:



Identity is associated with individual agency because it is related to the ability of the individual to shape her identity beyond the gaze and influence of powerful others. Those who advocate the defense of privacy against the threats of technology and social practice do so, in part, because of the belief that the “right to be left alone” is fundamental to the development of the autonomous individual. Identification on the other hand, is understood in the context of the exercise of power and authority. (Gandy, 2000, p. 2)

In other words, we can think of identity as something that is determined by an individual on their own (self-determination) or something that is ascribed to them. This ascription of identity may be done without the knowledge of the person (subject) or it may be assigned to them against their will. In the normal functioning of society it is quite natural and necessary for both types of identity to be constructed. Reputation, for example, is part of a person’s identity that is socially determined and is critical to the functioning of any complex society (Solove, 2007; Allen, 2003; Posner, 1978).

Although the term identity is highly controversial, it is possible to define it in a neutral manner that is inclusive of both self-determined and ascribed entities. The definition comes from the NRC ID card primer IDs, *Not that Easy* (Kent & Millet, 2002):

Identity: The identity of X according to Y is a set of statements believed by Y to be true about X....Identity generally refers to a set of information about X, especially in the context of a particular identity system. (p. 12)

Using this definition, we can see that substituting Y for X, identity can be self-defined. My identity, as I would like to believe it, consists of the total set of true statements that I can make about myself. As we begin to explore the implications of this definition in detail, we will begin to see how an identity is ultimately a discursive object whose subject is the identified person.

Our identity, this collection of statements, can be a mixture of statements that we produce intentionally, statements that are produced by others about us, and statements that represent traces of mediated interactions we have engaged in the past. There at times may be disputes about this identity, with more powerful discourses often winning out over weaker ones, regardless of any

inherent truths contained in the entities themselves. In the past, individual citizens of modern civilizations have been able to construct multiple identities both serially and in parallel, in a manner entirely harmonious with the stability and security interests of society. Parents, for example, have had one identity they shared with their children and another they shared with each other. Employees have a particular identity they share with an employer and a different identity they share with old college friends.

#### SYSTEM OF RECORDS

The term “system of records” is used in the U.S. Privacy Act of 1974 to describe “a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.” A record, as the Privacy Act defines it, “means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual” (5 U.S.C. § 552a ).

This term has been criticized by some within the computer science field as unclear, inaccurate, and out of date:

Quite unlike a system of records, today’s databases are heterogeneous, having complex structures determined by the purposes for which they were constructed, and plagued by difficulties in semantic interoperability because of different vocabularies and different perspectives on the use of the data. Further, they are often maintained by multiple sites, are capable of linkage of records across databases, and may not be under the control of a single authority. This makes the application of existing law and administrative procedures problematical. (Duncan, 2003, p. 6)

Similarly, Clarke (1994) points out that “information system” is a better, general term which is understood to include not only records, “but also computer-based processes, manual procedures

and man-machine interfaces” (n.p.). Clarke concludes “[t]his article therefore avoids the term “system of records” and suggests that legislative draftsmen do likewise” (n.p.).

While these critiques certainly have validity, the term “system of records” remains the language of U.S. law and policy and has a certain value despite its entailments and assumptions. While the term “record” implies a type of data object that is standardized and controlled by a particular institution, there is a great deal of data out there containing personally identifying information that is not part of an institutional record system. While it is true that the term does not address this greater ontological range of personal data elements, any state dossier system will necessarily involve a “system of records” to facilitate the retrieval of data linked to a particular person. As with any fixed definition, the term does remain open to certain semantic games. Some agencies have avoided the Privacy Act requirement for notice of any time a “new” SoR is planned by claiming that although the database itself may be new, the records of which it is comprised were produced within other systems of records subject to their own notice requirements. Clarke argues for the term “set of records,” a suitably vague term to indicate a grouping of records held under the auspices of a single institution; but again, this is not the current legal term in use.

#### PERSONAL INFORMATION

It is important, for the analysis that follows, to make clear distinctions between three terms that are often conflated in academic and policy literature: *personal information*, *personally identifying information*, and *personally identifiable information*. We can define personal information as any information that was produced by or describes some aspect of a person. That information may later be used to develop an understanding of an individual person or human behavior in general. Personal information, though it is drawn from specific individuals, is not necessarily linked to them. If someone participates in an anonymous computer survey about particular health behaviors and no data is stored related to their IP address, their personal data is

very likely to be anonymous data. Within this broad class of personal information, when the record includes specific text that specifically points to that person, such as a social security number or driver's license, then this constitutes personally identifying information. Other information, such as a phone number or address, is also specific enough to be considered personally identifying information, since it will correspond to one or only a handful of people. Personally identifiable information describes records of personal information where it may be possible, depending on the specific information and the resources of a particular actor, to trace the information back to the specific individual who was sourced. So called anonymous information is personal information that has no chance of being traced back to the individual in question. As we will see, the range of definitively anonymous personal information is quite small.

Philips (2004) distinguishes between three different forms of identification: *lexical*, *descriptive*, and *indexical*. Lexical identification is the assigning of a name to a particular class of thing, like the Latin names given to individual plant species. Descriptive identification, on the other hand, assigns attributes to an entity that distinguishes it in some way from another entity. Telling a police officer that we saw someone with blonde hair and a limp is descriptive identification. Finally, indexical identification points to a specific entity. Pointing at someone running down the street and yelling "stop thief" is indexical identification, but so is assigning a unique tag such as a social security or driver's license number.

When we talk about personally identifiable information instead of personally identifying information, we are generally talking about a distinction between indexical and descriptive identification. If description is detailed enough, it can make indexical identification possible, but only when the combined attributes in the description represent a unique combination not possessed by others. This is why it is important to consider very carefully the actual data stored in a supposedly anonymized record.

It is helpful in this context, to add a fourth class of identification between descriptive and indexical information, which we might call contextual indexical identification. This type of identification is more than simple description, because it is used to distinguish a particular entity, a customer, from all other entities that an institution deals with, but it does not necessarily facilitate the identification of the individual outside the context of the particular business relationship. Consider, for example, if Amazon stored a database of individual customer book purchases indexed by a customer number, rather than a driver's license, credit card, or social security number. If this database were leaked and accessed by someone outside the company, this book purchase information (most likely) could not be linked to specific individuals and joined with other data such as their medical or employment history.

Determining whether a data set, even if contains only contextual, indexical identifiers, is truly anonymous, is not a simple task. Although a number of models for anonymity within a data set have been developed by computer scientists, including k-anonymity (Sweeney, 2002), l-diversity (Machanavajjhala et al, 2006) and t-closeness (Li et al, 2007), many of these models have been shown to be vulnerable to different types of attack, particularly when the attacker has access to additional sources of personal data.

## PRODUCTION

Cognition is the most socially conditioned activity of man, and knowledge is the paramount social creation. (Fleck, 1979, p. 42)

A great deal of work in the academic field known as “social construction of reality” has challenged the notion that “facts” exist out there in the world waiting to be discovered. Latour & Woolgar (1986), for example, have shown that seemingly objective scientific facts are not discovered but are thoroughly constituted by the material setting of the laboratory. Summarizing

the early work of Fleck on the *Genesis and Development of a Scientific Fact*, Golinksi (2005) explains:

The social character of knowledge is revealed by the circumstances of its production within a specific interactive community ... which sustains a distinctive mode of reasoning.... ( p. 32)

I do not wish to enter the active discourse over the relative merits of the social constructivist critique of modern science, but the insights they offer are particularly useful when considering the world of personally identifying information. Personal information is not simply, “out there.” It is produced within specific social, institutional, and technological contexts. Without first the production of information, its “objectivation” (Berger & Luckmann, 1966) into material form manifested in our common world, information cannot be collected.

The production of information occurs at the moment a symbolic representation takes physical, persistent form in a medium of storage, the moment that information becomes bound to an artifact. Two people talking on the telephone, in this definition, are not producing information; rather, they are communicating. If, on the other hand, the telephone company is secretly recording the conversation (storing it, for example, on a reel-to-reel tape that is then labeled and stored away in a file cabinet) a form of information has been produced. My use of “production” then, is intended to highlight two aspects of personal information that tend to be hidden within the more common, “collection” frame. First, that the storage of otherwise “immaterial” information within a specific medium is contingent, dependent upon specific institutional and individual choices. Second, that the information itself encodes a particular symbolic structure implicated within a larger structure of meaning that creates as much as it captures regarding the data subject.

As part of the exploration of personal information production within state dossier systems I will use the terms “site” and “logic” of production. The term “site of production” has multiple meanings depending on context. It may refer to the institutional site of production of a particular

system of records, such as the IRS or the FBI. It may refer to the actual physical location of record production, whether it occurs within an office at the subject's place of employment or inside a police car on a state highway, or a combination of physical locales that may be involved in the production and storage of electronic records. Consideration of the site of production includes an examination of the record itself and its attributes, not only the physical form it takes (paper and ink, stone, compact disc) but the specific attributes of the symbols that comprise the specific media object (in other words, the content of the record) and the discursive formation of which they are a part. Questions about *what* is produced, *who* produces it and *where* they produce are also critical to understanding the sites of production.

The term, "logic of production," refers primarily to both the how (specific procedures and affordances) and the why (criteria, justification) of production. It helps us consider the specific schema which are used to determine specific moments of production. What is the justification for producing PII within this particular context (at this particular site)? Is the justification based on the utility of the information or its potential profit value or something else? What specific criteria for producing PII records are given to the producers and do they end up following these criteria? How does the development and diffusion of information technology impact how PII records are ultimately produced (or not produced). Other aspects of the how of production might include specific training scenarios given to potential producers, such as state agents for programs connected to specific systems of records like suspicious activity reports. How is a particular system of records configured to produce records? What situational conditions must be present for production to be triggered? How is the production of the record afforded? What resources facilitate production? Is it produced by a human agent with specific training or is it automatically generated within a technologically enabled system?

Within any state dossier system there are multiple sites and logics of PII production. As we examine a specific case, we want to be able to speak to the most important sites and logics and underline what might be “problematic” about them. That is, particular logics of production may be unsound and may afford extremes in practice that are ultimately contrary to the public interest.

#### DATA SHADOW/DOUBLE

The term “data shadow,” the totality of individually identifiable data left behind by people as they go through their daily lives, was first coined by privacy scholar Alan Westin (1967). Although the phrase did not catch on initially, its increasing relevance in the Internet age has led to its resurgence, and the emergence of a new, more ontologically distinct notion, the “data double” (Haggerty & Ericson, 2000).

We can think of the difference between data doubles and data shadows in terms of discourse theory, where the data double is the object produced within a particular discourse and is the collection of statements about an individual within that discourse that constitutes their identity. Poster (1990) was one of the first communication scholars to talk about this discursive relationship between databases and individual identity via what he called the Superpanopticon:

... the discourse of databases, the Superpanopticon, is a means of controlling masses in the postmodern, postindustrial mode of information....the population participates in its own self-constitution as subjects of the normalizing gaze of the Superpanopticon. We see databases not as invasion of privacy, as a threat to the centered individual, but as the multiplication of the individual, the constitution of an additional self, one that may be acted upon to the detriment of the “real” self without the “real” self ever being aware of what is happening. (Poster, 1990, pp. 97-8)

The additional self of which Poster speaks is discursively constructed (drawing on Foucault’s (1972) theory of discourse) through a process known as interpellation. The process generates the subject out of the space of relations emerging from the objects of the particular discourse. For example, in the discourse of psychiatry, concepts such as manic depression or



libido establish a space of relations in which individuals are constituted as mental patients. Poster points out that the process of interpellation via database is much different in character than in the classroom or the doctor's office, in which the interpellated subject is present and (at least somewhat) able to influence the process:

With databases, most often, the individual is constituted in absentia, only indirect evidence such as junk mail testifying to the event. Interpellation by database in this respect is closer to the instance of writing, with the reader-subject being hailed by an absent author. But here again there are important differences: from the standpoint of the person being interpellated, the writer is known, even if only as a writer, and is an individual or finite group of individuals. The reader very often intentionally selects to be interpellated by the particular author, whereas in the case of computer databases that is rarely if ever the case. Interpellation by database is a complicated configuration of unconsciousness, indirection, automation, and absentmindedness both on the part of the producer of the database and on the part of the individual subject being constituted by it. (p. 187)

This process of interpellation which leads to the creation of the data double takes place within a single database, a single system of records. The data double has become the preferred focus of attention in place of living, breathing people, as institutional agents make decisions about them. Individuals remain at least partial producers of their data doubles and can exercise certain choices that impact their size and character. This control, however, is highly correlated with one's available economic resources, and can be reversed into suggestibility; a process Zarsky (2003) calls the "autonomy trap."

The data shadow, on the other hand, is a more diffuse entity than the data double. One's data shadow is the totality of all data one might associate with an individual. While the shape and depth of a sun shadow is a straightforward combination of the person, the ground and the light behind them, the production of one's data shadow is far more complex, with a far more dubious connection to the subject herself. It comprises all personally identifying data indexed to a unique individual in systems that may or may not interconnect, data that includes errors and willful misrepresentations. At any given moment, the data double in use during institutional praxis is

unlikely to contain anywhere near this totality of information (though it certainly may contain errors). In the ideal dossier system, however, all data from an individual's data shadow would be accessed in the process of interpellation, yielding a data double of unusual detail and scope.

Data doubles, in and of themselves, are often useful and necessary things. Without them, much of what we take for granted in the modern world, such as buying things on credit, doing business with people with whom we have had no prior relationship, drawing unemployment insurance, getting customized book recommendations, or getting accepted into an educational institution without first having to fly there in person, would be impossible, or at the very least, much more difficult. We cannot expect private or public institutions to stop producing data doubles without dramatic, often negative impact on our daily lives. At the same time, data doubles can be the cause of great injustice and inequality. As data doubles grow in importance in our lives, they begin to erode the significance of our own selves:

The notion of individual biographical truth, already weakened by current epistemologies, is further marginalized by pragmatic institutional choices, where both actuarial calculations and data-matching procedures constantly produce real consequences for individuals represented by their ersatz doubles. (Los, 2006, p. 86)

#### AFFORDANCE

Originally developed by Gibson, the concept of affordance addresses the physical properties of an object or environment and its impact on the possibility for action. In Gibson's theory, physical objects and features, when considered in conjunction with physiological attributes of specific animal species, afford certain actions. Trees afford climbing for squirrels. Tree branches afford perching for owls. Chairs afford sitting for people. Key in Gibson's original argument is that affordances emerge out of a relation between physical characteristics of the environment and those physiological capabilities of a particular species; they are not inherent in the environment or physical objects. The very conception of affordance requires the presence of

both nodes in the relation. This protects the analyst from independently assigning intrinsic properties to external objects without the participation of living beings and thereby falling into the “essentialist trap.”

Hutchby (2001) extends Gibson’s concept of affordance to include not just features of natural and man-made objects in the environment but our relationship to technology of all kinds:

I want to propose an approach to the study of technologies and social life which offers a reconciliation between the opposing poles of constructivism and realism. This involves seeing technologies neither in terms of their ‘interpretive textual’ properties nor of their ‘essential technical’ properties, but in terms of their affordances (Gibson 1979). I will argue that affordances are functional and relational aspects which frame, while not determining, the possibilities for agentic action in relation to an object. In this way, technologies can be understood as artefacts which may be both shaped by and shaping of the practices humans use in interaction with, around and through them. This ‘third way’ between the (constructivist) emphasis on the shaping power of human agency and the (realist) emphasis on the constraining power of technical capacities opens the way for new analyses of how technological artefacts become important elements in the patterns of ordinary human conduct. (p. 444)

In the course of this dissertation I will make use of the concept of affordance in two senses: first, as particular kinds of communication technologies develop, they can afford the production and exchange of personal information; second, the presence of certain kinds of records within a state information system affords, though does not necessarily determine, certain types of behavior.

## THE PROBLEM

Laudon (1986) introduced the term “dossier society” to frame the problem of database surveillance specifically in terms of state power and the aggregation of personal data into large-scale information systems:

From the individual’s point of view, the most significant characteristic of the dossier society is that decisions made about us as citizens, employees, consumers, debtors, and supplicants rely less and less on personal face-to-face contact, on what we say or even what we do. Instead, decisions are based on information that is held in national systems,

and interpreted by bureaucrats and clerical workers in distant locations. The decisions made about us are based on a comprehensive “data image” drawn from diverse files.

From a technical and structural view, the central characteristic of the dossier society is the integration of distinct files serving unique programs and policies into more or less permanent national databases....

From a political and sociological view, the key feature of the dossier society is an aggregation of power in the federal government without precedent in peacetime America. From a cultural view, the dossier society is one which exposes thousands of officially selected moments in your past to confront you with the threads of an intricate web, revealing your “official life,” the one you must live with and explain to whatever authority chooses to demand an explanation. (pp. 3-4)

The state dossier society that Laudon warns about here is facilitated by the nexus of two systems: 1) a national system of identification and 2) one or more systems of records for the storage and management of personal information. These two components work synergistically to enable a “dossier system” in which the production of personal information expands in an accelerating feed-back loop. As state bureaucracies and large scale private corporations have become more effective at producing and enforcing the use of personal ID, they have learned to check claims directly against their own data rather than having to take the individual at his or her word. Not only do these cards facilitate direct access to the data in state databases, but they lead directly to the production of more information.

At the beginning of the 20<sup>th</sup> century there were few organizations which could be counted on to generate authoritative personal information on a mass basis. Even birth certificates probably covered no more than half of those being born. And without sources of “breeder documents,” the bases for generating further documents were weak.

As sources of authoritative personal data available for direct checking grow, however, the costs of mass surveillance drop. Indeed, viewing the broad sweep of historical change, we conclude that *mass surveillance through personal documentation feeds on itself*. The more important events in life entail production or consumption of personal documentation, the more feasible it is to institute effective surveillance through direct checking based on such data. Imaginative administrators of surveillance organizations are constantly seeking new uses of personal data in these ways. (Rule et al, 1983, p. 232)

As states build information systems that can potentially create extremely detailed and comprehensive data doubles, the identity and self-determination of the individual subject

becomes endangered. In the dossier society, these files, retrieved or updated upon presentation of an identity card, become an integral part of how powerful institutions discriminate in their treatment of individuals, informing decisions regarding their right to travel, hold a job, or receive medical treatment or government assistance. The culmination of this process of mass surveillance through personal documentation is the national identity card. National identification systems enable the production, management, and retrieval of PII via their links to associated databases and national registries and, through this process, the social sorting of individuals into categories of privilege and exclusion. They represent the most visible component of a state's surveillance infrastructure and enhance its power (Stalder & Lyon, 2003). According to Lyon (2007), national identification systems "may turn out to be the single most significant development of information systems for governance, globally" (p. 111).

A national ID card system in principle offers a government a single means of entry into the myriad databases that currently incorporate personal records of many different kinds. Analogously (in some ways) to the so-called Clipper Chip, which would have given the U.S. government sole and ultimate access to encrypted on-line messages, national electronic ID cards enhance the power of the nation state. Such systems facilitate searches throughout those flexibly integrated discrete databases that currently — in the USA, Canada, and the UK — currently have no such single key. Of course, it is correct to argue that in today's increasingly networked information infrastructures no single, integrated national ID card is needed for such comprehensive searches to be made possible. The unique identifier would just make such searches easier. (Stalder & Lyon, 2003, p. 90)

Much academic work today that problematizes the growth of personal information databases focuses on the impact of private institutions such as retailers and insurance companies on the life chances of individuals. Gandy (1993) has shown how the growing corporate practice of gathering information on individual consumers has resulted in the growing marginalization and exclusion of significant sectors of the society. Turow (2006) argues persuasively that the growing trend of database marketing is "beginning to engender new forms of envy, suspicion and institutional distrust" (p. 19). Andrejevic (2007) shows us how the explosion of personal

information allows private company and state institutions to steer its information subjects into certain desirable patterns of behavior, a phenomenon Zarsky (2003) originally labeled the “autonomy trap.”

The problem of the state dossier system is potentially much more dangerous to the public interest than issues related to private data mining and the interpellation of consumer identities. The state has unique authority to collect and produce records of personal information and to use physical force based on this information. Further, states appear to have a bureaucratic tendency (Weber’s rationalization) to expand records of personal information to the limit of one’s data shadow and work to expand the data shadow itself through the promotion and promulgation of ubiquitous ID systems and technologies. The data double produced by a state which commands access to a particularly wide range of personal information is likely to push back on its subject in ways that less detailed, more narrowly constituted data doubles would not. The dossier system does not produce the subsequent oppression, but it at least affords it and is often understood as direct expression of that oppression.

It is vital here to distinguish between the “state dossier system” as a problematic configuration of state information systems that traffic in personal information and those configurations which are necessary for the state to function as intended. In cybernetic terms, the basic function of the state is to act as regulator of the social system, to keep the system within a stable state of homeostasis. Part of that duty is being able to rapidly shift resources to citizens of the state who may most need them and to be able to respond to human threats such as crime, natural disasters, or economic dislocation quickly. In order to perform its job, the regulator must have continuous feedback from the system it is regulating.

A dossier system, on the other hand, is a kind of generalized data aggregation that cannot be successfully defended on the grounds of legitimate state functions such as the provision of resources or management and negotiation of risk. Dossier systems emerge when coverage begins to expand beyond obvious dangerous populations to include innocent citizens. Dossier systems emerge when built in bureaucratic logics of rationalization are not countered by public awareness, legal arguments and technological fixes in the public interest. Dossier systems emerge when the public is not educated to the dangers of the loss of anonymity from the state.

One can think of a state dossier system as an extreme form of domestic intelligence system in which there is an excess of PII on an excess of individuals, overloading intelligence agents to the point where their jobs become more difficult and the potential grows for increasing instances of needless, oppressive interactions between members of the public and state agents, ranging from delays in boarding airplanes to physical abuse, confinement, torture and even death. The boundary between a domestic intelligence system and a dossier system, however, is not clear cut. There is a grey area where different scholars and policy analysts might disagree as to whether the extent of personal information included within a data system is justifiable given the state's role in managing their risk of terrorism or whether it is contrary to the public interest.

### THREE KEY DANGERS

The following section advances the argument that state-centered dossier systems pose three key dangers to society: 1) political repression; 2) the loss of individual autonomy and gradual surrender of self-determination; and 3) poorer adaptability in the social system as a whole due to the loss of "cultural variety," a form of biodiversity.

### (1) POLITICAL REPRESSION

Information contained on subjects of state dossier systems is often collected and acted on for political reasons, to cultivate particular classes of actor while marginalizing and hindering others. While this negative effect of the SDS system is clearly associated with historical regimes such as Nazi Germany and Soviet Union, and with contemporary regimes like the People's Republic of China, it is important to recognize the history of dossier systems and political repression in the U.S., covered most comprehensively in Donner's (1981) epic study of U.S. intelligence programs of the 20<sup>th</sup> century.

Political intelligence is a by-product of diplomatic and military conflict, and despite its domestic provenance, is marked by a similar hostility toward the intelligence target (itself a revealingly hostile term of art). Like its military model, political intelligence reductively divides the world into patriots and traitors, friends and enemies, us and them. Even though the target is an American national, engaged in lawful political activities in his own country, he is viewed in an adversary context. Life in a relatively open society, which boasts of its freedom, makes the target enormously vulnerable when his politics come under hostile investigation by a secret police unit with an anti-subversive mission. Nowhere else in our society is the private life of unprotected individuals subjected to such intensive scrutiny by an agency of the government, and for reasons unrelated to any familiar and recognized government function such as law enforcement. The individual's vulnerability is intensified by the secrecy of the probe and the knowledge that even if no "derogatory" information is developed he or she will become a permanent file subject. Inevitably, surveillance and even the fear of surveillance on the part of those not actually monitored produce a pervasive self-censorship. (p. 6)

For many educated individuals, Donner's claim is extreme and of doubtful validity. Evidence of intelligence abuses by successive administrations in the 20<sup>th</sup> century is chronicled in considerable detail in the 1973 Church Committee reports.<sup>9</sup> Even over the past ten years, as will be detailed in subsequent chapters, numerous incidents of dossier production and harassment of peace and civil rights activists have been noted by investigative journalists and subsequently confirmed by the government's own investigations.

---

<sup>9</sup> See chapter 3, p. 91.



Political repression is but one, acute form of discrimination that can emerge from the state dossier system. Below, I consider the more general problem of self-determination and autonomy.

## (2) INDIVIDUAL AUTONOMY AND SELF-DETERMINATION VS. DISCRIMINATION

... control over personal information is control over an aspect of the identity one projects to the world, and the right to privacy is the freedom from unreasonable constraints on the construction of one's own identity. (Agre & Rotenberg, 1997)

“Autonomy” connotes as essential independence of critical faculty and an imperviousness to influence. But to the extent that information shapes behavior, autonomy is radically contingent upon environment and circumstance. The only tenable resolution — if “autonomy” is not to degenerate into the simple, stimulus-response behavior sought by direct marketers — is to underdetermine environment. Autonomy in a contingent world requires a zone of relative insulation from outside scrutiny and interference — a field of operation within which to engage in the conscious construction of self. The solution to the paradox of contingent autonomy, in other words, lies in a second paradox: To exist in fact as well as in theory, autonomy must be nurtured. (Cohen, 2000, p. 1424)

To fail as a poet — and thus, for Nietzsche, to fail as a human being — is to accept somebody else's description of oneself, to execute a previously prepared program, to write, at most, elegant variations on previously written poems. (Rorty, 1990, p. 28)

The more individuals lose control over the production of “statements” (propositions about them) that comprise their identity, the more they surrender their own self-determination. Much academic work today has focused on this problem in the context of private institutions such as retailers and insurance companies. Gandy (1993) has shown how the growing corporate practice of gathering information on individual consumers has resulted in the growing marginalization and exclusion of significant sectors of the society. Turow (2006) argues persuasively that the growing trend of database marketing is “beginning to engender new forms of envy, suspicion and institutional distrust” (p. 19). Andrejevic (2007) shows us how intensifying asymmetric flows of personal information both from consumers to private corporations and from citizen subjects to their states afford a higher degree of malleability and suggestibility among the general public. The consumer citizen is shaped into desirable patterns of

behavior by what appears to them to be the exercise of free choice, via mechanisms just beyond the horizon of awareness.

Discrimination is “the end result of the social construction of difference in the pursuit of profit and social control” (Gandy, 1995, p.37). The difference can be understood as the particular categorical distinction upon which an institutional decision is made. Any categorical assignation contained in a particular set of identity records implicates a much more detailed set of propositions which all members in that group share. This association within the identity may be willingly adopted by the subject or it may be ascribed to them. In democratic court situations, the citizen has a chance to be aware of certain categorical ascription (you are a criminal) and to defend against them. When these categories recede into the background beyond human awareness, injustice will multiply and continue to evade traditional schema of social redress.

Zarsky (2003) has coined the term “autonomy trap” for scenarios he has drawn up that show how marketing firms might use data about their customers to “lead them” into certain purchases. In this situation, the consumer is the target of a cybernetic system directed at changing their behavior. Not only might categorized and classified consumers find certain market options discouraged or not available to them, but they might be “steered” into certain patterns of consumption that are not in their interest. The autonomy trap “creates a setting in which the individual is lead into a new market and is purchasing a product she has no initial interest in, as opposed to being overpriced for a product she initially wanted to purchase.” The autonomy trap operates via a complex feedback loop between the commercial sector and the consumer.

Zarsky relates the hypothetical story of an individual who wishes to quit smoking. Mr. Orange, who usually buys his cigarettes through an online retailer, purchases a “nicotine patch” to help him kick the habit. The online retailer, upon receiving information about this purchase, sends

him a set of email vouchers for free cigarettes and, at the same time, sees to it that ads promoting smoking are served more frequently to the web pages he visits. Mr. Orange, who has something less than an iron will, is thrilled by the free cigarettes and puts his newly acquired nicotine patch on a back shelf in his medicine cabinet.

How this loss of autonomy manifests itself is not always easy for the subject to perceive. He or she may be simply feel unlucky. While it is quite possible to experience the oppression of a dossier system directly, decision making can be integrated into cybernetic algorithms in such a way that it is hidden from the subject. The man in Zarsky's autonomy trap may fall back into his smoking behavior none the wiser that it was his personal information that did him in. The subject's behavior is gently prodded and nudged into the desired norm.

In the context of the state dossier system, this loss of autonomy and discrimination is potentially much more acute and unavoidable. The state can draw on a much broader range of data to inform the process, thereby claiming higher authority for its particular categorical ascription. The state also has available to it a much broader range of life altering decisions and actions on data subjects (including incarceration and execution) than does the private firm, with far fewer options for "exit."

How many categorical distinctions and distinct watch lists emerge, or already exist today, within the local, state and federal domestic intelligence assemblage is difficult to know or predict. Within the market, the diversity of these categories goes far beyond the green, yellow and red categories most commonly associated with federal passenger risk assessment programs for the airline system. The Claritas PRIZM system's "66 demographically and behaviorally distinct" psychographic categories derived from demographic, consumer behavior, and geographic data, for example, include "Money and Brains," "New Empty Nests," and "Mobility Blues." There are

no laws at either the state or federal level that would limit the number of such risk categories and associated treatment protocols that might emerge.

As is detailed in chapter 4, records of suspicious activity increasingly produced within the United States by agents of local, state and federal governments can include unvalidated statements and have no minimum standards regarding the degree of supporting evidence. These reports may then flow into federal risk assessments leading to the ascription of a higher than normal risk category on a watch list of some form that then triggers less than respectful treatment protocols and the subsequent loss of economic and social opportunities. These practices appear to be growing largely outside traditional schema of due process, such as the right to know the charges against you and the evidence that led to the charges.

It is important to be clear about just what the problem is here. To say that the social construction of difference, as a general practice, produces this discrimination would argue against all human knowledge. As I will explain in more detail below, social systems theories such as cybernetics and complexity theory highlight the value and significance of informational variety and its role in system regulation and adaptability. Critical are the logics of how this informational variety is produced, where it is stored, and whose interests it serves. Today, both citizens and consumers are surrendering much of their autonomy and self-determination because they do not participate and often cannot even see the creation and ascription of these categories.

### (3) CHILLING EFFECT AND THE PRODUCTION OF CULTURAL VARIETY

Well established within legal and political discourse is the notion that obtrusive surveillance may lead to a chilling effect in which people are afraid to speak their minds. The chilling effect has a negative impact on the quality of deliberation, limiting the chances for innovations and insights to emerge. Foucault has elegantly described the manner in which

continued surveillance can cause subjects to internalize norms of their institutions. Records of personal information that persist can extend this normalizing force beyond a particular moment of observation, as they may be attended to and enrolled in a potentially life changing decision making algorithm any time in the future.

The potential for durable expressions and logs of activity to persist may have a dampening effect on symbolic expression and “deviant” behaviors that can produce innovation. In other words, extending the logic of the “chilling effect” to its more systemic implications, the extent and scope of dossier systems is inversely related to the production of “cultural variety.” As cultural variety decreases, so does the overall social systems capacity for adapting to environmental change and other instabilities.

In purely biological terms, the case for conservation of diversity, biodiversity, is well established. For example, Tillman & Downing’s (1994) study of the North American grasslands demonstrated that systems with more biodiversity recovered more quickly from drought than those systems with less diversity. In the 1990s, scholars began to suggest that one could map the inferences about ecology and diversity from the domain of biology to that of language and culture. As this work has gained momentum, it has begun to carve out its own discursive identity, what Maffi (2005) has called the emergence, of the field of “biocultural diversity.”

The abundance of species and language systems both play key roles in evolution and survival, a reflection of more general cybernetic principles such as Ashby’s *Law of Requisite Variety*. The Law of Requisite Variety answers the question: how much internal variety must a regulator have available within a system to maintain order in the face of outside disturbances? Ashby argues that there must be at least as much variety within the system as there is variety in the potential for disturbances. Heylighen (1992) develops and partially restates Ashby’s law in his

*Principle of Selective Variety*: the greater the number of configurations (states) a system can take, the greater the possibility that one of the configurations will be retained as a solution to the threatening instability. It follows logically, then, that systems with a wider range of possible solution configurations to attend to are better able to deal with a wider range of problems than those systems with less variety.

The difficulty, however, lies in measuring cultural variety. The field, to date, has largely relied on a very basic measure of linguistic/cultural variety: the number of individual languages within a social boundary. Language diversity is used by Harmon (2002) explicitly as a proxy for the richer “cultural variety.” Other proxies for cultural variety have included the number of religions and identified ethnicities within a national census.

Notwithstanding these challenges, and the importance of making further distinctions within this category (such as between linguistic and epistemological variety,) one can understand the general proposition that excessive surveillance systems have a normalizing function that dampens overall variety. The key question is whether this variety is useful, harmful or simply irrelevant.

An effective surveillance system would dampen harmful variety such as violent crime and pandemic disease while preserving or enhancing the development of knowledge and ideas. While this makes sense in the abstract, achieving such an ideal will involve the creation and destruction of variety that is not so easily labeled either way. Heylighen argues, in fact, that we cannot distinguish between useful and non-useful variety and merely select from available variety on a random basis until something “works.” At that point we select this bit of variety and forget others.

The problematization of the state dossier system holds that the indiscriminate creation and storage of personally identifying information specifically constrains the development of knowledge and ideas, both useful and non-useful, while simultaneously failing to protect the citizen subjects from the bad variety of terror and crime. State dossier systems suffocate discursive/expressive margins where significant new ideas and innovations might emerge, thus limiting the overall system's ability to adapt to environmental changes.

## DISCUSSION

What does it matter if state institutions collect information on citizens if nothing is done with the information other than to protect them from terrorists? Recalling my cybernetic definition of surveillance, it is important that we consider the full circle, from feedback to regulation. It is not just the collection of information about environments and their objects, but actions based on this information that matter. A surveillance system in which masses of personal information are recorded but ignored by the state is a vastly different condition from one where wide ranges of personal data are regularly attended to and acted on, especially when those actions are oppressive. As we can see above, however, these actions may not be directly visible to the subject while still having tremendous impact on their lives. Even if our present government does not use the information it collects for anything but narrowly targeted counter-terrorism operations, the simple presence of wide ranging data on innocent Americans affords possible future scenarios in which this information is abused. State dossier systems afford, do not determine, oppression.

Although the history of state dossier systems in the 20<sup>th</sup> century shows us that citizens very much felt the oppression of the dossier system, both physically and psychologically, one could imagine a 21<sup>st</sup> century form in which the average citizen were entirely unaware of their

oppression, gently nudged and guided into a particular norm that seemed to them to be a life largely self-determined.

I should make it clear that I am not arguing for the right of an individual to have complete control over their own identity creation. Clearly, reputations have great social utility. Nevertheless, as individuals become deprived of spaces in which to experiment with new ideas and practices, or begin to see themselves more as objects of scrutiny than as autonomous beings, they will fall within narrower ranges of life expression. They will innovate less. Not only does this take away from the power and freedom of the individual life, it also impacts the viability of the social system as a whole. The social system will inevitably support a narrower range of individuals and thus have accessible to it fewer resources for innovation and the resolution of unanticipated problems.

#### RESEARCH QUESTIONS

So far in this chapter, we have established a new frame for surveillance as a social problem, focusing on the emergence of state dossier systems as a precursor to government oppression and totalitarianism. This dissertation focuses on the following primary research questions that flow from this problem frame: *What are the primary components of state dossier systems and what are their interrelationships? What are the forces that propel and hinder the construction of state dossiers systems today? How do states justify their construction and how do publics resist them?* While the dissertation largely assumes that expanding dossier systems afford more authoritarian and totalitarian government configurations that manifest in tense, negatively-valenced interface between the state and the public, it will also provide examples of how Americans are already experiencing these negative effects. The primary goal of this dissertation is to gain enough understanding of this ongoing, real-world U.S. case to facilitate better policy analysis and new legal regimes that can help minimize the likelihood of totalitarian scenarios in



the future. As part of this process, and with the instrumental use of the Chinese case for juxtaposition, I will offer a set of more general terms, a “problematizer’s toolkit” so to speak, for effective discourse illuminating the ins and outs of state dossier systems.

#### FOUR DRIVER’S OF STATE DOSSIER SYSTEMS

In chapter 1 (p. 11), I introduced Lyon’s four major strands of surveillance theory. On the basis of this extant theoretical work, I have identified four factors that serve as significant drivers of state dossier systems: *law*, *technology*, *political economy* and *public sentiment*. Two of these drivers, technology and political economy, are drawn directly from the theoretical strands that Lyon identified. The other two, law and public sentiment, can be understood as driving factors identified within the overall nation-state strand of surveillance theory. Since technology and political economy have already been described in detail above, here I focus only on the remaining drivers: law and public sentiment.

#### LAW

Although the topics of law and public sentiment are addressed directly within the theory of political economy, they warrant distinct research and analysis categories. Laws have great power to both enable and constrain state surveillance in ways that can only become clear in focused legal analysis. As Balkin (2003) puts it, law “is a form of cultural software that shapes the way we think about and apprehend the world” (p.8). Legal doctrines establish facts as well as systems of rights and responsibilities associated with the social actors and their objects (Tiller & Cross, 2005). In the U.S., the Fourth Amendment of the Constitution has long been one of the most significant constraints on state surveillance practices. How this amendment has become close to irrelevant in the world of 21<sup>st</sup> century communication (Sundstrom, 1998; Solove, 2002) is best understood via focused legal analysis that leaves broader political economic questions largely in the background.

The force of law in a particular nation state depends on its political context and history. While Chinese modern society has typically had little respect for law, the political system has been undergoing great change in recent years. China's legal system is in the midst of transition from what the state calls "too much emphasis on the rule of person and insufficient emphasis on the rule of law" to a system modeled after Western democracies, "from supremacy of the power to supremacy of the law" ("Human Rights Achievements in China," 2000, n.p.). China's legal system has continued to gather strength (Peerenboom, 2002), a trend which began to accelerate as the country approached the Olympics (Harris, 2007). This expansion of law serves more to constrain the activities of businesses and lower level government institutions than party elite. Although law plays much more of a role in society than it did a decade or more ago, legal code is often unclear and contradictory, and often fails to act as a constraint on the activities of law enforcement. Articles 242 and 245 of the General Principles of Criminal Law criminalize unauthorized searches of homes and reading of private mail respectively, but law enforcement officials can issue search warrants on their own authority.

#### PUBLIC SENTIMENT

Public sentiment is also an important topic in need of individual study. Although state and private actors will always try to influence public opinion in ways that political economy can certainly explain, public sentiment can be observed and measured on its own terms and may not always cooperate with elite attempts to mold it.

Within the life of the generation now in control of affairs, persuasion has become a selfconscious art and a regular organ of popular government. None of us begins to understand the consequences, but it is no daring prophecy to say that the knowledge of how to create consent will alter every political calculation and modify every political premise. (Lippman, 1922)

Whether or not a political system of government has specific channels for the public to exert its will, such as democratic elections, public sentiment usually enters into the policy

decisions of governments (Kluegel, Mason & Wegener, 1995). Public sentiment can have powerful effects on the political capital a given state may have to engage in various kinds of surveillance practices and can influence both the creation and interpretation of laws.

Public sentiment can be measured using different kinds of proxies, from formal public opinion polls, to activity in the court system, to public protests and demonstrations, and can also be discerned in the very conceptualization of privacy and its value compared to other social values, such as security and accountability. Public opinion polls are conducted regularly in both China and the U.S., but we must be cautious not to assume that poll data in either country can give us some truly objective notion of what the public thinks. The results of polls are highly dependent on the questions that are asked, and, in the U.S., the decisions on what questions to ask are often made by private corporations with particular agendas.

Businesses that depend on unfettered access to personal and transaction-generated information will be especially concerned to represent the public as unconcerned about, or supportive of, businesses having that access (Gandy, 1993). They will use estimates of public opinion to help convince policy makers of the wisdom of supporting the policy opinions that they prefer (Herbst, 1993). As a result, skillful public relations often explain the disparity between what the public actually believes and the character of their beliefs as they are represented in the press (King & Schudson, 1995) (Gandy, 2003, p. 287).

To speak of public sentiment in China is itself a complex matter. There are vast differences of experience and world view between China's urban, largely coastal residence and the rural peasants. Most polls do not reflect the views of this much larger economic class. Public opinion research is quite new in China and there remain questions about the validity of the data. Urban polls rarely account for migrant workers, a sizable population of the big cities. Guo Liang of the Chinese Academy of Sciences, for example, notes that a traditional Chinese cultural bias to tend toward the mean (Confucianism) is likely to decrease the utility of questions based on Leichert scales. Still, methods have been improving and Chinese citizens are increasingly willing to speak their mind (Tang, 2005).

Further, mass media outlets including newspapers and Web sites in China have conducted and published public opinion polls that appear to constrain certain policy positions of the state. There are certainly boundaries which such polls may not cross, but the range of tolerable questions has been expanding by fits and starts. Though perhaps gaining strength in recent years, public opinion has always had to be reconciled with state policy initiatives.

It is difficult to imagine that any regime, democratically elected or not, can sustain itself for very long without taking public opinion into consideration. The Chinese rulers, long before the invention of modern elections, compared public opinion to the river and the state to the boat — a boat that, if misguided, could easily be overturned (*shui neng zai zou, yi neng fu zou*). (Tang, 2005, p. 198)

It seems unlikely that PR firms in China have developed to the level of sophistication they have in the U.S. to influence the production and distribution of poll data within policy discussions, but of course there remain other concerns about just how much we can trust the data. Nevertheless, we will see in chapter 6 that published public opinion and public demonstrations seem to have successfully challenged state plans and policy initiatives.

#### INTERACTIONS BETWEEN THE FOUR DRIVERS

The four factors, far from mutually exclusive, exhibit a great deal of interaction. For example, the production and distribution of new technologies may afford new kinds of practices that become unpopular with the public. Strong public sentiment against these emerging practices may result in the passage of laws constraining such practices. This is a simple but largely accurate description of how the U.S. Privacy Act of 1974 emerged after academics and activists became concerned about the potential abuse of computer systems and databases which were just gathering momentum at that time (Solove, 2006). On the other hand, if it moves in the opposite direction, public sentiment can result in very different laws.

## METHOD

Before providing some notes on the research process for this chapter, I would first like to acknowledge and briefly describe a few major research efforts that I place within the U.S. state dossier system (SDS) problem frame. That is, they are works that directly address and contribute to our understanding of the U.S. SDS. Although these texts may use different terminology and different methods, they all have been major contributions to the subject and help highlight important ways in which the present study differs (and thus may serve to contribute new perspective).

With a sweeping account of U.S. intelligence abuses gathered in the course of years of data collection, Donner's (1980) *Age of Surveillance* describes the height of abuses by U.S. domestic intelligence agencies and other federal departments from the 50s to the 70s. Though published within a few years of the Church and HEW committees, the Privacy Act of 1974 and FISA, Donner remained quite pessimistic that the role of intelligence as a tool for quelling political dissent could be effectively constrained. Donner's research method, which involved, "collecting materials from a wide range of sources — press clippings, legal documents and court records, pamphlets, interviews, reports, government publications, to name the salient ones — dealing with official attacks on non-conformity," (p. xi) is similar to my own method, though it used a different sampling procedure (as I will explain below).

Laudon's (1986) definition of the problem and his term "dossier society" is very close in meaning to my phrase "state dossier system." Laudon's research method, however, was to focus on a specific SoR, the FBI's National Crime Information Center (NCIC), also known as the national Computerized Criminal History (CCH) system, and then interview local police, prosecutors, judges and other decision makers who would act as users of the FBI's then proposed

system. This study does not focus solely on one SoR or one institution. A more recent work in this area by David Sobel (2002) uses the term “national identity system” (NIDS). While it appears that he is interested in not only a system of identification but the potentially massive set of personal records that it could contain, I want to distinguish the notion of a national ID system from the larger question of an overall dossier system. The dossier system comprises not only some form of ID system and its supporting record systems (such as to verify the unique holder of a driver’s license or birth certificate), but a potentially much more vast universe of PII that the state has the power to produce, acquire and act on. As I will show in the pages that follow, this includes, perhaps most importantly, the state’s vast apparatus of intelligence gathering. While domestic intelligence apparatuses are understood to take place within an environment of legal constraint within this U.S. democracy, these constraints now appear to be weaker than at any time in the past two centuries.

Solove’s (2004) *Digital Person* is perhaps the most significant book related to the SDS problem in the past decade, but its focus is more general, on the general availability of personal data within both public and private spheres, rather than focusing specifically on the state’s specific orientation to PII as Laudon and Donner do. It is an excellent resource for studying law relevant to the SDS problem frame.

Shorrock’s (2008) *Spies for Hire* is another major contribution to the SDS problem frame. Its coverage of the intimate relationship between the private sector and U.S. intelligence agencies is important and highly detailed. It documents the tremendous size of the private sector that contributes to the U.S. intelligence system and points out that it is largely free from legal constraints and affords widespread opportunity for corruption. This dissertation does not focus on the role of private companies. Rather, it looks more specifically at the state’s role, the relevance

of law, policy and specific state practices that can make possible (that afford) such a significant private sector role.

#### COMPARISON-CASE STUDY HYBRID

This case study approaches this problem of the U.S. SDS from an initially very broad frame — in essence, the basic model of the dossier system as consisting of two subsystems: 1) ID systems and 2) systems of records. It focuses primarily on the state rather than private actors and avoids selecting particular institutions or well known SoRs as the starting point for research.

The research design for this study is based primarily on the case study, but with some important differences. First, rather than begin with a specific database or a specific institution, which the researcher might then examine by traveling to the site of the particular database and interviewing direct participants (or even more direct observation akin to an ethnography,) I use publicly available, electronic documents as the general data source and approach them first based on abstract concepts. Second, the analysis makes important instrumental use of cross-national comparison as a tool for developing a general vocabulary of state dossier systems and gauging the intensity of the U.S. SDS problem.

#### COMPARISON

The idea of directly comparing media systems has been developed most extensively in the work of Hallin & Mancini (2004). The observation of differences and similarities between media systems, they argue, can help to clarify thinking about each system, challenge culturally and geographically situated assumptions, and reveal important gradations in what may mistakenly be viewed as black and white concepts. The notion of “objective” news, for example, so widely associated with the American media system, was challenged by Hallin & Mancini’s (1984) own

comparative work between Italian and U.S. television journalism. American newscasters appeared to engage in far more interpretation of news compared to their Italian counterparts.

Ferdinand Braudel (1980) was one of the first sociologists to point out the benefits of this kind of analysis in understanding what otherwise may appear to be very familiar contexts:

Live in London for a year and you will not get to know much about England. But through comparison, in the light of your surprise, you will suddenly come to understand some of the more profound and individual characteristics of France, which you did not previously understand because you knew them too well. (p. 37)

A binary comparison of nation states with very different histories, political systems and cultures provides an ideal format for this kind of research. As Dogan & Pelassy (1990) note in their highly influential work, *How to Compare Nations*, “the perception of contrasts makes researchers sensitive to the relativity of knowledge and consequently helps liberate them from cultural shells” (p. 9). A binary comparison, they add, “permits a kind of detailed confrontation that is almost impossible when the analysis encompasses too many cases” and “makes possible a study in depth” (p. 127). In his address to the American Sociological Society, president Melvin Kohn (1987) stated that cross-national comparisons were “potentially invaluable” and “grossly underutilized” (p. 713).

In more general terms, Marshall McLuhan (1964) argued that direct juxtaposition of otherwise unrelated elements can lead scholars to unexpected insights and analytical clarity of their objects of study that may otherwise be elusive:

“Interface” refers to the interaction of substances in a kind of mutual irritation. In art and poetry this is precisely the technique of “symbolism” (Greek “symballein” — to throw together) with its paratactic procedure of juxtaposing without connectives. It is the natural form of conversation or dialogue rather than of written discourse. In writing, the tendency is to isolate an aspect of some matter and direct steady attention upon that aspect. In dialogue there is an equally natural interplay of multiple aspects of any matter. The interplay of aspects can generate insight or discovery.



## CASE STUDY

Although it is common for cross-national comparisons to be designed to contribute to the development of general theory or to isolate particular causal factors in social systems, the rationale also derives from its basic utility in adding analytical clarity through contrast, as a way of gaining deeper insight into the real-world cases in question. The case study approach — an empirical investigation, using multiple sources of evidence that targets a contemporary phenomenon within its real-world context when the boundaries between the phenomenon and context are unclear (Yin, 1984) — is the second component of this methodological hybrid.

There is a tension in case study analysis between what Stake (2000) calls *intrinsic* and *instrumental* studies. In the intrinsic case study, the researcher is interested in the particular case itself, without the need to develop general understanding of a generic phenomenon. In the instrumental case study, the case is chosen “to provide insight into an issue or redraw a generalization” (p. 437). Stake laments the common assumption that case studies are valueless if they cannot provide instrumental value beyond understanding the target case itself. “Damage occurs when the commitment to generalize or to theorize runs so strong that the researcher’s attention is drawn away from features important for understanding the case itself” (p. 439). In the present study, even though China’s role is primarily instrumental, both cases of interest are large in size and scope and important to understand in their own right.

## DATA GATHERING AND SELECTION

Data gathering and analysis for this dissertation is heavily influenced by Checkland’s (1981) Soft Systems Methodology (SSM). SSM is designed for the investigation of systems that are not well defined and whose internal structures are undergoing continual change. Using Checkland’s method, the researcher not only analyzes the real-world situation in terms of its systemic features, he/she also incorporates the systems concept into the very process of

investigation. That is, the research method forms its own feedback loop, between the real-world situation that is being investigated and the conceptual model that is developed to illuminate its dynamics. Rather than create a rigid analytical framework in which all data are forced to conform, the research process is the primary driver of analytical resolution.

Case study research is resonant with SSM, often commencing without predetermined analytical categories; instead, categories are allowed to emerge naturally in the process of investigation (Stake, 1995). Cross-national comparisons, on the other hand, are expected to begin with clear categories or dimensions on which the comparison will be based (Dogan & Pelassy, 1990). The amount of data a researcher might collect in a cross-national comparison could be so voluminous as to be overwhelming. Beginning with categories or dimensions for research helps guide, channel and limit the research process. As a result, this study works both with pre-determined categories (the four drivers of dossier systems, described above) and an open-ended process of model building. Comparisons between the two countries are made along these four dimensions, while more intrinsic aspects of each individual case were allowed to emerge in the process of data gathering.

#### BOUNDING THE DATA RETRIEVAL PROCESS

Given the potential volume of data involved, case study approaches must have some technique for limiting the data set that will be then subject to analysis. As Stake (2000) notes, after a particular case has been chosen, “there are subsequent choices to make about persons, places and events to observe (p. 447).” Because these case studies are focused on publicly available documents rather than on site research, the process for making these choices is distinct enough to merit detailed description here.

How one bounds the research process when the available documents are in very large number is one of the challenges for researchers fully engaging Internet research methods. In her work *Virtual Ethnography*, Hine (2000) points out that traditional ethnographers rarely had to consider the issue of data bounding in any significant way, since the remote locations they chose had their own physical boundaries and settings which constrained the flow of information. In the absence of such boundaries, Hine suggests that the ethnographers focus “on flow and connectivity rather than location and boundary as the organizing principle.” (p. 64)

Although this dissertation is not an ethnography, research is bounded in a similar fashion, in the process of following links and associations between documents based on their lexical and semantic content. It is useful to consider this problematization as in part the construction of an identity (the state dossier system) via the linking or propositions. Since the term “state dossier system” itself is an abstraction, it is not possible to simply draw together all available documents which contain the phrases “state dossier system” and extract their propositions. Such documents would be very few in number and represent a poor distribution of available information. It is also not possible to simply collect all documents which in the abstract speak to this general concept, because the researcher would be quickly overwhelmed in information exceeding his or her ability to assess.

The vast majority of the data for this dissertation were collected from two general pools of electronically accessible documents: 1) real-time news streams using RSS feeds and 2) active, “archival” searches using both Google and Lexis-Nexis. Archival in this sense does not necessarily mean that the documents are stored in a formal archive, only that they have been

stored and are electronically accessible. The choice of documents was driven by an iterative process of keyword selection and snowball sampling with increasing semantic specificity.<sup>10</sup>

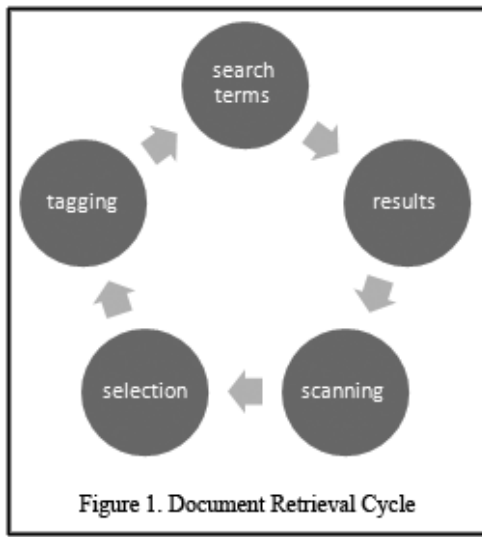
#### DOCUMENT RETRIEVAL CYCLE

Publicly available documents serve as the source of data for this study. Documents are collected and analyzed according to an open but systemic process which operates in five cyclic steps: 1) search terms, 2) results, 3) scanning, 4) selection and 5) tagging. Each cycle generates a set of documents that comprise the data for each case study. The cycle continues as decisions are made to refine or alter research questions to better understand the case on its own terms.

---

<sup>10</sup> By semantic specificity, I am referring to the relative generality or specificity of a word or phrase as it might appear in a subsumption hierarchy or hierarchical category tree, such as the Tree of Porphyry, developed by the Greek Philosopher Porphyry in the 3rd century AD as part of a commentary on Aristotle's categories. Subsumption hierarchies, or definitional networks (Sowa, 2002) "emphasize the subtype or is-a relation between a concept type and a newly defined subtype." The network defines the rules of inheritance, showing how properties in more general categories are related to their subtypes. The earliest known network of this type was the Tree of Porphyry, drawn by the Greek philosopher Porphyry in the 3rd century AD as part of a commentary on Aristotle's categories. The network included the "substance" category at the top of the hierarchy, defined as the "supreme genus," with increasingly specific subcategories, such as "living" and "mineral" or "animal" and "plant" branching out below. A more modern version of the definitional semantic network is the Open Directory Project, "the largest, most comprehensive human-edited directory of the Web." The directory facilitates the navigation of information and knowledge on the web through its classification in a hierarchy of general to specific categories.

Although the Open Directory Project is an attempt to classify all knowledge, one can easily imagine a similar kind of hierarchical directory focused on state dossier systems, where words and terms move from generally applicable across large-scale cases to highly specific and context dependent. The more specific words and terms are necessary for the detail of a case study while the more general terms provide context and abstractions that help the researcher position the cases within a broader phenomenological umbrella.



*Search terms:* A combination of keywords and phrases that reflect a particular moment of the searching process, the evolution of which is described in detail below.

*Results:* total set of documents retrieved in search, ranked (by provider) in relevance or chronology. From this total set of results, the percentage of documents that can be subsequently scanned varies according to the number of documents and their relevance to the research question.

*Scanning:* Resulting documents are scanned from the top, beginning with title and source, indicated on the results page. Articles and news items which do not fit the definition of dossier system are immediately discarded. Documents with relevant titles and respected sources are then retrieved and scanned directly for content. In cases where available documents exceed my ability to read them, retrieval continues until the novelty rate of retained documents begins to fall, suggesting adequate data coverage of the case node has been reached.

*Selection:* Authoritative documents that fit within the broader conceptual and case boundaries and add new and useful information are retained. Articles found that do not add new data to the emerging picture of the dossier system for that country are discarded.

*Tagging:* Retained documents are tagged using multiple keyword tags to facilitate their subsequent integration in analysis and next stage document searches. Tags are based on relevant keywords and concepts that represent emergent case nodes. Tagging includes both the use of the web-based *delicious*<sup>11</sup> application and a local data archive indexed and organized using the *Freemind*<sup>12</sup> mind mapping application. Tagging incoming data with

<sup>11</sup> *Del.icio.us* allows me to store the URL, title, brief notes, and multiple keyword tags for each item that I choose to retain.

<sup>12</sup> *Freemind* is a knowledge organization tool that allows the storage of documents and other electronic files within multiple, nested nodal hierarchies. As case nodes were identified in the course of case study analysis, data was stored under those nodes within a *Freemind* mind map, facilitating the retrieval of all documents linked to a particular case node. Any given document may be stored within multiple node hierarchies - case nodes, data source, driver - increasing its subsequent "findability". The term "findability" was coined by information architect Peter Morville

multiple tags/codes, rather than forcing it into a specific category, facilitates the article's subsequent retrieval at multiple points of analysis and allows associations between data objects to emerge naturally.<sup>13</sup>

*Search terms:* A new set of search terms is generated based on analysis of interpretation of existing document set, including the construction of narratives and identification of knowledge gaps. Resulting documents continue to expand the document set, building understanding of the overall dossier system case and the specific case nodes identified in the course of research.

#### LOGIC OF SEARCH PATHS

In addition to using the rather standard method of citation sampling, where document collection follows notable, formal citations within the bodies of already collected texts (Krippendorff, 2005), I noted the presence of particular, semantically specific, words and phrases within these documents which could stand as important sub nodes for further research. These phrases were not common phrases, but unique in some way that characterized important documents and helped identify more targeted paths for further keyword searches. Amazon.com calls these “statistically improbable phrases” (SIPs). I will refer to this method later in the dissertation as the “SIP snowball.”

SIPs are used as part of Amazon's “Search Inside!” service to facilitate both the location and characterization of its books in stock.

To identify SIPs, our computers scan the text of all books in the Search Inside! program. If they find a phrase that occurs a large number of times in a particular book relative to all Search Inside! books, that phrase is a SIP in that book.

SIPs are not necessarily improbable within a particular book, but they are improbable relative to all books in Search Inside!. For example, most SIPs for a book on taxes are tax related. But because we display SIPs in order of their improbability score, the first SIPs

---

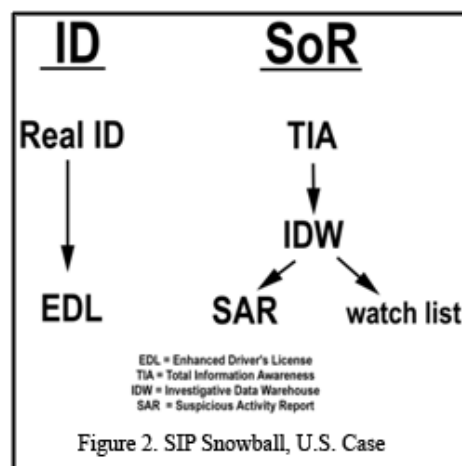
(2005) and refers to the attributes of an object (physical or digital) that make it more or less findable. For physical objects, this might include distinctive colors or shapes, or the specific location that happen to be at a particular time. For digital objects, this would include their titles, keywords associated with them, and links pointing toward them.

<sup>13</sup> For example, let's say I retrieve an article "NSA Teams up with the Chinese government to limit Internet anonymity." After quickly scanning the article, I might decide to assign it the following tags: surveillance (default), NSA, China, U.S., anonymity and tech. Later, on, in the process of analysis, I might want to retrieve all articles I have retained that deal with the concept of anonymity, or those articles that deal specifically with China and anonymity, or all those articles that deal with technology as a driver of dossier systems. The delicious tool allows me to retrieve stories that fit any keyword combination.

will be on tax topics that this book mentions more often than other tax books. For works of fiction, SIPs tend to be distinctive word combinations that often hint at important plot elements (“Amazon.com, What are Statistically...” 2009, n.p.).

At the beginning stages of research, keywords are very general and the incoming data is very broad. The identification of particular SIPs within the course of document analysis lead to the establishment of important “case nodes” for the individual case studies. The earliest SIPs end up being (historical, conceptual) touch points for the researcher to understand this large problem domain, but their individual significance is hard to measure early on. As research under a particular SIP progresses, other SIPs appear within this narrower class of documents, which can either help add to understanding of the particular case node or point to other, potentially more significant/fruitful nodes of investigation.

The diagram to the right represents, in most basic form, the major signposts of my SIP snowball research flow for the U.S. case as it unfolded. Search began based on the two subsystem concept of the general SDS model: ID systems and systems of records (SoR). As should be apparent in the diagram, the ID research was more straightforward than the SoR research. The initial keyword/SIP, RealID, remained of useful focus for the duration of the project, with the Enhanced Driver’s License (EDL) emerging as an SIP of likely future significance.



As emergent terms are entered back into the document search process, the set of retrieved documents fluctuates with the specificity of various terms. In general, the longer and more complex the search term, or the more semantically specific or improbable the term is, the lower the number of results. Terms may be either semantically or lexically derived. In other words,

search terms may be considered close to one another in meaning, or they may be discovered within documents that have already been, retained, stored, scanned and tagged. Statistically improbable phrases connected to emergent case nodes facilitate more efficient search. In the course of the research process, I made decisions about which particular SIP case nodes would anchor the research process. *Appendix A* provides a more detailed narration of this process.

### SOURCES OF DATA

Rather than employing on site or ethnographic research common to case studies, this dissertation relies exclusively on publicly available documents. Increasingly, government documents produced at both the state and federal levels are available online. Since the Government Printing Office Electronic Information Access Enhancement Act of 1993, online access to U.S. federal documents including the *Congressional Record* and *Federal Register* has been required by law. Virtually all major U.S. newspapers are accessible online, with extensive archives available either directly on the newspaper web site or via database services such as Lexis/Nexis or Proquest. In China, online accessibility of government documents was formalized with the initiation of the 1999 Government Online project. Most of the country's current legal code is available on line in Chinese, often with English language translations available. Newspapers of records are available online and are generally archived at least 10 years back.

The Chinese government today does not have the same laws for public release of information that the United States has. It is not legally required to publish "Privacy Impact Assessments" of new programs or notify citizens about any new database that is expected to contain personally identifiable information. Further, there is considerably less leeway among journalism institutions as to their targets of investigation and reporting. As a result, there is a much lower volume of information produced by Chinese institutions that directly address the development and current configuration of the state dossier system. Nevertheless, a considerable



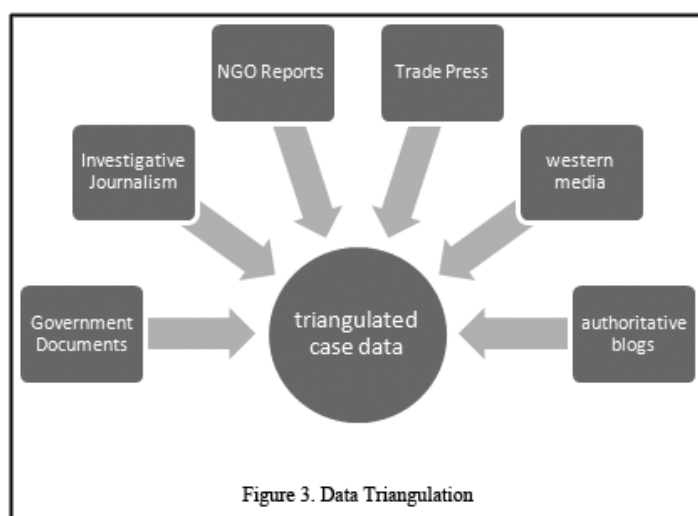
amount of information is still available. Privacy and anti-surveillance NGOs see China as the epitome of an Orwellian surveillance state and this spend a great deal of their own resources to gather and disseminate data. Further, the Chinese government itself willingly makes much of this information available.

For the China case, research focused on English-language source data. While I am fluent in Mandarin Chinese, opening the data gathering to Chinese language material would have dramatically raised the volume of incoming data while slowing analysis time. Available English language material, including official government news sources, NGO reports, Western investigative journalism, academic journals, books, and authoritative blogs, all of which I evaluated based on more than seven years of personal experience within the Chinese IT industry<sup>14</sup>, provided a complete enough picture of the system today to, at the very least, serve its instrumental role as a suitable comparison case and reference point for the United States.

---

<sup>14</sup> From 1996 to 1998 I was the senior Internet consultant for the Xiamen Xindeco Corporation. I oversaw all web related operations, including the production of the award winning website ChinaVista.com and helped bring the company to a successful listing on the Shenzhen stock exchange. During this three year period I interacted frequently with government officials including public security agents assigned to the public Internet. I later founded, obtained venture capital financing and served as CEO of VirtualChina.com. Although the company closed its doors shortly after the 2000 dotcom crash, VirtualChina.com was once a well known player in the China Internet industry and is the subject of a 2000 Harvard Business Case VirtualChina.com: The Building of a Virtual Community. Between 2001 and 2003, I continued to consult for Chinese Internet companies while living in the Xiamen Special Economic Zone.

## BREAKING DOWN DOCUMENT TYPES



A wide range of documents were found and stored. I break down these documents according to seven general categories: 1) government documents; 2) investigative journalism; 3) NGO reports; 4) trade press; 5) western media; 6) academic scholarship and 7) authoritative blogs. U.S. Government documents, which comprise roughly 1/3 of the acquired material for the U.S. case, can be further broken down into multiple categorical schemes, such as the originating government department or the document type. Documents included System of Records Notices (SORNS) and Notices of Proposed Rulemaking (NPRMs) published in the U.S. *Federal Register*, congressional testimony available from the *Congressional Record*, departmental reports such as those from the DOD Inspector General or more general research and accounting departments like the GAO and the Congressional Research Service (CRS). Chinese government documents can be broken down into state run media, public opinion surveys, national and regional laws, and any other documents available in the public record.<sup>15</sup> For a more extensive breakdown and list of key sources see *Appendix B*.

<sup>15</sup> Examples would include documents such as a Public Security bureau letter to Yahoo requesting the personal information of a particular Yahoo account or the published findings of the associated court case.

## DATA ANALYSIS: ASSESSMENT

I am making inferences about the dossier systems in each country based on publicly available documents. The degree to which the representations of these documents match the reality of the situation of interest is an obvious question. On what basis can I claim to make valid inferences about these systems based on public documents, rather than first-hand investigation of the systems themselves? Clearly, direct investigation of the systems themselves would be preferable but impractical for a number of reasons. Most importantly, at the outset of the U.S. case study, I had not yet chosen a specific database or system of records to target for research, making it impossible to indentify a specific institutional or physical location to conduct such a firsthand search. Second, it would be highly unlikely that the U.S. or Chinese governments would provide me the kind of access to such a system given the implications for national security.

Given the nature of the systems in question, it is certain that entire databases that store and analyze personal information are kept secret from the public with little or no published information indicating their existence. At the same time, in the case of both the U.S. and China, publicly available data does describe real systems whose configuration and use can tell us a great deal.

Saiz and Simonsohn (2007) have shown that the relative number of online documents discussing a particular phenomenon can be used as a proxy for its actual occurrence in the world. Comparing the frequency of occurrence of the word “corruption” associated with states in the U.S. and other counties, they found that high frequency states and countries correlated strongly with other available measures of corruption, such as the Transparency International (TI) index. Based on this validation of their method, Saiz and Simonsohn offered the first ever city by city index of corruption in America. Though clearly much corruption in any given country goes in the

darkness beyond public scrutiny, enough of this activity makes its way to public light such that it is possible to make inferences about the relative degree of the problem from country to country.

This dissertation operates on a similar assumption, that although I am no doubt missing certain aspects, certain components of the dossier system in each country, I am able to gather enough information from each country to assess the intensity and character of the problem in question. Since I am looking to do more than measure simple intensity — to explore the character of these systems — I cannot simply measure the frequency of stories related to dossier systems. Instead, I must evaluate propositions about these systems contained within these documents. As Dibble (1963) has pointed out, historians and social science researchers must be circumspect when making inferences from different types of documents and not simply take the propositions contained therein at face value. There is a dichotomy between documentary evidence and the facts or events external to the documents themselves that can vary widely with the type of document and the facts to be established.

Propositions within certain U.S. governments documents detailing specifics of certain record systems such as “system of records notices” (SORNs) published within the *Federal Register* were taken at face value. That the Automated targeting System (ATS) exists, is designed to assess risk of air travelers, and makes use of particular public and private data sources, is accepted on the documents legal authority alone. Public statements by officials denying the existing of a particular system, on the other hand — for example, Chertoff denying that the U.S. government has a central database storing information on U.S. citizens — are considered with more skepticism.

Propositions contained within works of investigative journalism, no matter the reputation of the news source, are evaluated and ideally triangulated with other sources before accepting the

enclosed propositions as representing accurate details of the system in question. For Chinese sources, certain government documents, such as the announcement of a new record or ID system, are also taken at face value. As I mentioned above, I also leverage over seven years of personal experience within the Chinese IT industry, which included direct interactions with public security officials, to judge the validity of investigative reports or other, more controversial government statements.

As is illustrated in the two tables below, the multiple source categories inform research and analysis for each selected case node and serve to triangulate key claims. The first table shows the seven basic types of documents retrieved in the left hand column and then lists important case nodes for both the U.S. and China cases along the top row. The case nodes are addressed in detail in the text of this dissertation. All case nodes draw data from multiple document types.

Data type	U.S.: Real ID	SAR	China: Hukou	Dangan	2 <sup>nd</sup> gen ID
Gov Docs	X	X	X		X
Journalism	X	X		X	
NGO Reports	X	X	X		X
Trade Press	X	X			X
Western media	X		X	X	X
Academic			X	X	X
Blogs	X				X

#### NOTE ON DIFFERENCES BETWEEN U.S. AND CHINA CASES

As we will see in the following chapters, research for the two cases proceeds on their own terms. In the Chinese case, the SIP snowball method was not as critical to the research outcome as it was for the U.S., due primarily to two factors: 1) the volume of data is considerably lower, in part due to the design of the study and in part because the state simply produces less publicly available information about its system; 2) the fact that China does indeed have a state dossier system is not really in dispute. There is no claim, from the state itself or any researcher,

that China does not now have a national ID system or a national population registry. There is little doubt that it has had and hopes to continue to have, detailed files on a large sector of the population. Searches to identify documents were thus more straightforward with the China case.

## CHAPTER 3: U.S. CASE, HISTORICAL CONTEXT

This chapter provides a brief historical and legal context for understanding the current configuration of the U.S. dossier system. As a largely heuristic device, and to simplify a very complex tapestry of law and policy that has impacted the evolution and configuration of the U.S. dossier system over the past several decades, I break down the U.S.'s "dossier history" into three phases.

In phase 1, a period lasting from the late 1920s until the mid 1970s, intelligence agencies monitored, produced files on, and interfered with the lives of hundreds of thousands of Americans for political reasons, free from significant oversight or practical legal constraint, under programs like COINTELPRO and CHAOS.

In phase 2, a period lasting from 1974 to 2001, initial horror at the degree to which the executive branch abused its domestic intelligence agencies motivated the legislative branch of government to make available a new set of "boundary resources," most importantly the construction of a "wall" between the government's policing and intelligence institutions and between individual agencies of the U.S. government. The flow of personal information across these walls was to be highly restricted and monitored by the judiciary branch. While these restrictions did appear to place some limits on what could be done, government agencies increasingly found ways around these general restrictions while Congress focused on sector-specific data protection laws.

Finally, in phase 3, beginning in 2001 and continuing today, this status quo was shattered after September 11<sup>th</sup>, where walls have become nothing more than barriers to "connecting the

dots”<sup>16</sup> that might protect America from its next attack. While vestiges of the initial boundary resources remain, such as the Privacy Act and contemporary institutional recognition of the principles of Fair Information Practice first articulated by the Department of Health Education and Welfare (HEW) Committee in 1974, there appears to be an emergent state belief that national security interests justify a basic state right, which citizens should trust them not to abuse, to access and produce information on everyone and everything. While the FBI has resumed its earlier (phase 1) role in domestic intelligence, these practices are expanding into the regular police force and, in fact, the broader private workforce.

There is a vast amount of constitutional, statutory and common law relevant to information privacy in the United States. This review focuses on those laws that are most important to understanding the problem of the dossier system and its two primary subsystems: *ID systems* and *systems of records*. While the laws are presented in chronological order, they could also be categorized in terms of their impact on the state dossier system; that is, whether or not the law is likely to constrain or afford problematic dossier system configurations. Laws that, at least on the surface, would appear to constrain state dossier practices include the Fourth Amendment, the Privacy Act of 1974, the Electronic Communications Privacy Act, and the E-Government Act. In this chapter I will discuss these laws, both their limitations and their strengths. Laws that would appear to most significantly increase the risk of dangerous SDS configurations are the USA Patriot Act and the Intelligence Reform and Terrorism Protection Act (2004). This section will also introduce two key legal distinctions: information in *storage* vs. *information* in *transmission*, and *content* vs. *envelope* information. Finally, this section will conclude with a review of the Fair Information Practices (FIPs), originally conceived by the HEW Committee and

---

<sup>16</sup> This was a "mantra" of the 9/11 Commission Report, a phrase which underlined its most forceful recommendation, that the barriers to information sharing imposed on state agencies and departments in the mid 1970s be dissolved within a new Information Sharing Environment (ISE). After all, it was a failure to "connect the dots" that had blinded the U.S. government to the attacks.



now accepted as general guidelines for handling PII. In the interest of brevity, I do not address sectoral laws targeted at narrow domains of PII collection such as the Health Insurance Protection and Portability Act (HIPPA), the Video Privacy Protection Act (VPPA) and Family Educational Rights and Privacy Act (FERPA). A more thorough analysis of laws impacting information privacy can be found in Solove (2006).

## PHASE 1

The Fourth Amendment, historically, has been the most significant legal constraint against the state penetrating the privacy boundaries of the average American citizen.

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The rights embodied in the Fourth Amendment, however, were obscured with the development of electronic communications technology. Juridical confusion can be traced back to 1928, with the Supreme Court decision *Olmstead v. United States*, which found that the Fourth Amendment did not apply to wiretapping a person's home phone. In the majority opinion, Chief Justice Taft wrote:

This Court has frequently said that the Fourth and Fifth Amendments should be construed liberally; but it is submitted that by no liberality of construction can a conversation passing over a telephone wire become a "house," no more can it become a "person," a "paper," or an "effect." (*Olmstead v U.S.*, 277 U.S. 438, 1928, n.p.)

Although Congress subsequently filled in the void with the 1934 Communications Act, expressly forbidding wiretapping without court order, such activity was considered outside the purview of the Fourth Amendment for the next thirty years. In 1967, *Olmstead* was reversed with the Supreme Court Decision *Katz v. United States*. In the majority decision, Justice Stewart asserted that the Fourth Amendment "protects people not places" and introduced the notion of a

“reasonable expectation of privacy,” which has been the guiding frame for legal interpretations of the Fourth Amendment ever since. In a nutshell, the reasonableness clause says that American citizens are protected whenever things they say or do would be expected by a “reasonable” person to be neither seen nor heard by someone else.

Despite this Supreme Court decision, it would be another seven years before widespread and often politically-motivated domestic intelligence gathering that had been going since the 1950s would see any significant legal constraints. During this time, America had essentially an active, insidious state dossier system which directly affected the lives of more than 100,000 Americans who had done nothing but use their First Amendment rights to assemble or speak or write in public. U.S. military, CIA, NSA and FBI members were actively opening and reading mail, eavesdropping on telephone conversations, and keeping files on large numbers of political dissidents.

COINTELPRO (an acronym for Counter Intelligence Program) was a series of covert and often illegal projects conducted between 1956 and 1971 by the FBI, under the direction of J. Edgar Hoover, aimed at investigating and disrupting dissident political organizations. COINTELPRO focused on infiltrating, disrupting, and/or marginalizing groups suspected of being subversive, including communist and socialist groups, the women’s movement, and civil rights organizations. The program remained secret until 1971, when a group of left-wing radicals calling themselves the Citizens’ Commission to Investigate the FBI broke into an FBI office in Media, PA, stole files and leaked them to news agencies (Davis, 1992).

By 1973, in the wake of the Watergate scandal, the newly energized Fourth Estate began to pay increased attention to the federal government’s excessive monitoring of and interfering with otherwise legitimate political activity:

... only four months later, *New York Times* reporter Seymour Hersh disclosed that the government's crimes went beyond Watergate. After months of persistent digging, Hersh had unearthed a new case of the imperial presidency's abuse of secrecy and power: a "massive" domestic spying program by the Central Intelligence Agency (CIA). According to Hersh, the CIA had violated its charter and broken the law by launching a spying program of Orwellian dimensions against American dissidents during the Vietnam War. The Times called it "son of Watergate."

These revelations produced a dramatic response from the newly energized post-Watergate Congress and press. Both houses of Congress mounted extensive, year-long investigations of the intelligence community. These highly publicized inquiries, headed by experienced investigators Senator Frank Church and Congressman Otis Pike, produced shocking accusations of murder plots and poison caches, of FBI corruption and CIA incompetence. In addition to the congressional inquiries, the press, seemingly at the height of its power after Watergate, launched investigations of its own. The *New York Times* continued to crusade against CIA abuses; the Washington Post exposed abuses and illegalities committed by the FBI; and CBS's Daniel Schorr shocked the nation by revealing that there might be "literal" skeletons in the CIA closet as a result of its assassination plots. (Olmsted, 1996, p.1)

## PHASE 2

The committees that Olmstead refers to helped paint a very clear picture of how the government had come to abuse its policing powers to enforce a political status quo. Frank Church's Senate investigation made it clear just how wide the specific abuses of the FBI, CIA, military and other agencies were in the 30s through the early 70s, while HEW provided a more abstract, philosophical approach to the problems of personal information held by the government, especially in the context of the emergent computer age.

### CHURCH COMMITTEE

Senator Frank Church (D-ID) chaired the "United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities" in 1975. Over a period of nine months, the committee interviewed more than 800 officials and held 250 executive and 21 public hearings, investigating widespread intelligence abuses by the CIA, FBI and NSA. The Church Committee's 14 reports, issued between 1975 and 1976, have been called the most thorough investigation of U.S. intelligence agencies ever released to the public. The reports

chronicled widespread intelligence abuses by the CIA, the FBI, and the U.S. military. The following excerpt from Book II, “Intelligence Activities and the Rights of Americans,” helps illustrate the degree to which U.S. intelligence activities were monitoring the lives of and keeping files on ordinary Americans:

United States intelligence agencies have investigated a vast number of American citizens and domestic organizations. FBI headquarters alone has developed over 500,000 domestic intelligence files, and these have been augmented by additional files at FBI Field Offices. The FBI opened 65,000 of these domestic intelligence files in 1972 alone. In fact, substantially more individuals and groups are subject to intelligence scrutiny than the number of files would appear to indicate, since typically, each domestic intelligence file contains information on more than one individual or group, and this information is readily retrievable through the FBI General Name Index.

The number of Americans and domestic groups caught in the domestic intelligence net is further illustrated by the following statistics:

— Nearly a quarter of a million first class letters were opened and photographed in the United States by the CIA between 1953-1973, producing a CIA computerized index of nearly one and one-half million names.

— At least 130,000 first class letters were opened and photographed by the FBI between 1940-1966 in eight U.S. cities.

— Some 300,000 individuals were indexed in a CIA computer system and separate files were created on approximately 7,200 Americans and over 100 domestic groups during the course of CIA’s Operation CHAOS (1967-1973).

— Millions of private telegrams sent from, to, or through the United States were obtained by the National Security Agency from 1947 to 1975 under a secret arrangement with three United States telegraph companies.

— An estimated 100,000 Americans were the subjects of United States Army intelligence files created between the mid 1960’s and 1971.

— Intelligence files on more than 11,000 individuals and groups were created by the Internal Revenue Service between 1969 and 1973 and tax investigations were started on the basis of political rather than tax criteria.

— At least 26,000 individuals were at one point catalogued on an FBI list of persons to be rounded up in the event of a “national emergency.” (Church, 1976, Book II, section 1, intro and summary)

The report also offers considerable details on how this abuse of personal information ended up impacting the lives of American citizens. Again, it is worth quoting a large portion of

the report, as it provides clear evidence that the U.S. during the 50s and 60s was already exhibiting many of the characteristics of a state dossier system:

Many of the illegal or improper disruptive efforts directed against American citizens and domestic organizations succeeded in injuring their targets. Although it is sometimes difficult to prove that a target's misfortunes were caused by a counter-intelligence program directed against him, the possibility that an arm of the United States Government intended to cause the harm and might have been responsible is itself abhorrent.

The Committee has observed numerous examples of the impact of intelligence operations. Sometimes the harm was readily apparent — destruction of marriages, loss of friends or jobs. Sometimes the attitudes of the public and of Government officials responsible for formulating policy and resolving vital issues were influenced by distorted intelligence. But the most basic harm was to the values of privacy and freedom which our Constitution seeks to protect and which intelligence activity infringed on a broad scale.

(a) General Efforts to Discredit. — Several efforts against individuals and groups appear to have achieved their stated aims. For example:

— A Bureau Field Office reported that the anonymous letter it had sent to an activist's husband accusing his wife of infidelity "contributed very strongly" to the subsequent breakup of the marriage.

— Another Field Office reported that a draft counsellor deliberately, and falsely, accused of being an FBI informant was "ostracized" by his friends and associates.

— Two instructors were reportedly put on probation after the Bureau sent an anonymous letter to a university administrator about their funding of an anti-administration student newspaper.

— The Bureau evaluated its attempts to "put a stop" to a contribution to the Southern Christian Leadership Conference as "quite successful."

— An FBI document boasted that a "pretext" phone call to Stokeley Carmichael's mother telling her that members of the Black Panther Party intended to kill her son left her "shocked." The memorandum intimated that the Bureau believed it had been responsible for Carmichael's flight to Africa the following day. (Church, 1976, section I.C.3)

The Church Committee recommended that the domestic intelligence functions of U.S. agencies and departments be dramatically curtailed, limiting the collection of U.S. domestic intelligence to the FBI and reducing its intelligence role to criminal activities and terrorism:

... the ultimate goal is a statutory mandate for the federal government's domestic security function that will ensure that the FBI, as the primary domestic security investigative agency, concentrates upon criminal conduct as opposed to political rhetoric or association. Our recommendations would vastly curtail the scope of domestic security investigations as they have been conducted, by prohibiting inquiries initiated because the Bureau regards a group as falling within a vaguely defined category such as "subversive," "New Left," "Black Nationalist Hate Groups," or "White Hate Groups." The recommendations also ban investigations based merely upon the fact that a person or group is associating with others who are being investigated (e.g., the Bureau's investigation of the Southern Christian Leadership Conference because of alleged "Communist infiltration").

The simplest way to eliminate investigations of peaceful speech and association would be to limit the FBI to traditional investigations of crimes which have been committed (including the crimes of attempt and conspiracy). The Committee found, however, that there are circumstances where the FBI should have authority to conduct limited "intelligence investigations" of threatened conduct (terrorism and foreign espionage) which is generally covered by the criminal law, where the conduct has not yet reached the stage of a prosecutable act. (Church, 1976, Book II)

In its 1976 final report, the committee proposed a "comprehensive legislative charter defining and controlling the domestic security activities of the Federal Government." While no legislation was passed, U.S. Attorney General issued a new set of FBI guidelines that largely resonated with Church Committee recommendations. Under the "Domestic Security Investigation Guidelines," (also known as the Levi guidelines) the FBI adopted a "criminal standard" (Shulsky and Schmitt, 1991) that would focus the bulk of its operations on specific criminal activities and not on open ended threats that tended to characterize the abuses of prior decades.

The Guidelines placed specific limits on techniques the FBI could use and distinguished three types of domestic security investigations: 1) preliminary investigations, 2) limited investigations, and 3) full investigations. The Guidelines provided that the FBI could commence a full domestic security investigation only on the basis of "specific and articulable facts giving reason to believe that an individual or group is or may be engaged in activities which involve the use of force or violence." (U.S. DOJ, 2005, September, ch. 2, sec. 3A)

Although Congress did not pass specific legislation restricting the domestic intelligence activities of the FBI, it did pass the Foreign Intelligence Surveillance Act (FISA) of 1978. FISA established a secret court responsible for issuing warrants for domestic wiretapping activity, comprising seven judges, appointed by the Chief Justice who serve for seven years.

It is of critical importance to understand the difference between the gathering of intelligence and a criminal investigation. I will use here the definition of “domestic intelligence” offered by the RAND Corporation (2008), in its recent white paper, “Reorganizing U.S. Domestic Intelligence.”

We define domestic intelligence as follows: efforts by government organizations to gather, assess, and act (see Figure 2.1) on information about individuals or organizations in the United States or U.S. persons elsewhere that is not necessarily related to the investigation of a known past criminal act or specific planned criminal activity. (Treverton, 2008, p. 15)

In his epic work, *Age of Surveillance*, Donner (1980) reflects on the role of intelligence in the state:

“Intelligence” is best understood as a sequential process, which embraces the selection of the subject (an organization or individual) for surveillance, the techniques, both overt and clandestine, used in monitoring the subject or target, the processing and retention of the information collected (files and dossiers), and its evaluation in the light of a strategic purpose (the intelligence mission). Intelligence also includes an activist or aggressive aspect, specifically designed to damage or harass the target. But whether formally classified as passive data collection or aggressive intelligence, the intelligence function is dominated by a punitive or proscriptive purpose. Even the selection of a target embodies a judgment of deviance from the dominant political culture. (p. 3)

Donner’s work, a detailed account of the domestic intelligence abuses in the U.S. from just after WWI until the early 70s, sees intelligence primarily as a tool of political coercion. In the years following the Church hearings, it was understood as general policy for agencies operating on U.S. soil to be constrained in their intelligence activities.

In reaction to the Church committee hearings, the FBI and other federal departments were constrained in domestic intelligence gathering. The FBI, under the new AG directive, moved away from intelligence and focused on criminal investigations. Heyman, in the passage below, describes the culture of the FBI just after the September 11<sup>th</sup> attacks and prior to its repurposing a domestic intelligence agency to fight terrorism.

The FBI's background as a law enforcement agency means that it has primarily emphasized reaction-capturing and prosecuting criminals after the fact-more than prevention. In cases where the FBI has, for example, infiltrated groups to prevent a crime, the focus again is on law enforcement and prosecution. A law enforcement agency is not accustomed to the jobs of providing warning, assessing vulnerabilities, or informing policy-makers. Rewards and incentives in the FBI have tended to be for law enforcement successes, and movement to an emphasis on intelligence successes has been halting. On the other hand, there are important synergies between the law enforcement and intelligence roles. The basic mechanisms of collection-surveillance, use of human sources, undercover operations, and review of records -are similar between the two disciplines, so many skills transfer from one to the other. But there are also differences, primarily that law enforcement conducts cases on activities one is generally already aware of; intelligence, by contrast, attempts to uncover things one was not aware of. (Heyman, 2008, p. 159)

#### HEW COMMITTEE

In 1972, then-Secretary of the Department of Health Education and Welfare (HEW) Elliot L. Richardson, appointed an Advisory Committee on Automated Personal Data Systems to explore the impact of computerized record keeping on individuals. The following year, the "Secretary's Advisory Committee on Automated Personal Data Systems" released what is now commonly referred to as the HEW report, entitled "Records, Computers, and the Rights of Citizens." The report focused more on the abstract, philosophical problems related to the government's use of personal information combined with the new affordances of electronic communication technology (specifically, computers), rather than recounting the specific abuses that had taken place to date that the Church committee report provides. The HEW report is a powerful articulation of the public interest in information privacy and the inherent dangers of states with too much power to traffic in records of personal information:

The report examines the characteristics and implications of a standard universal identifier and opposes the establishment of such an identification scheme at this time. After reviewing the drift toward using the Social Security number (SSN) as a *de facto* standard universal identifier, the Committee recommends steps to curtail that drift. A persistent source of public concern is that the Social Security number will be used to assemble dossiers on individuals from fragments of data in widely dispersed systems. Although this is a more difficult technical feat than most laymen realize, the increasing use of the Social Security number to distinguish among individuals with the same name, and to match records for statistical-reporting and research purposes, deepens the anxieties of a



public already suffused with concern about surveillance. If record-keeping systems and their data subjects were protected by strong safeguards, the danger of inappropriate record linkage would be small; until then there is a strong case to be made for discouraging linkage.

Concern about abuses of authorized access to “integrated” data systems maintained by State and local governments can have a particularly debilitating effect on people’s confidence in their governmental institutions. Ambitiously conceived integrated systems, no matter how secure technically, may have the effect of blurring, either in fact or appearance, established lines of political accountability and constitutionally prescribed boundaries between branches of government. When different branches arrange to share an integrated data-processing facility and its data, the executive usually will operate it. This happens partly because operational functions are normal for the executive, and partly because executive agencies usually have more experience with computer systems. It leads people to fear, however, that the needs of executive claimants may be met before the needs of legislative bodies and the judiciary. The priority system for allocating computer support will, of course, look fair on paper, but in practice the result may often be to shortchange the passengers on the system in favor of the driver.<sup>5</sup> The recent development of mini-computers, much cheaper than the big systems of only five years ago but of comparable power, is providing an attractive economic alternative to large integrated systems. Large systems, however, are also becoming less expensive and there is no assurance that they will not become even more so as the result of new technological advance. (U.S. HEW 1973, Summary and Recommendations, n.p.)

The most lasting contribution of the HEW report has been the *Code of Fair Information Practices*, basic principles which have influenced the passage of numerous privacy laws worldwide, including the Privacy Act of 1974.

1. There must be no personal data record-keeping systems whose very existence is secret;
2. There must be a way for an individual to find out what information is in his or her file and how the information is being used;
3. There must be a way for an individual to correct information in his or her records;
4. Any organization creating, maintaining, using, or disseminating records of personally identifiable information must assure the reliability of the data for its intended use and must take precautions to prevent misuse; and
5. There must be a way for an individual to prevent personal information obtained for one purpose from being used for another purpose without his or her consent. (U.S. HEW, 1973, p. viii)

The Hew Committee also made specific recommendations dealing with the use of social security numbers as indexes for agency systems of records containing personal information.

We recommend against the adoption of any nationwide, standard, personal identification format, with or without the SSN, that would enhance the likelihood of arbitrary or uncontrolled linkage of records about people particularly between government or government-supported automated personal data systems. (quoted in Smith, 2004)

Unfortunately, as we will see, the ambitious code it presents as the basis for a general legal policy affecting both the public and private sector did not survive the process of political compromise that concluded in the Privacy Act of 1974. The Act, though regularly referred to in name today by government institutions that traffic in PII and who pledge their compliance, is really best thought of as set of guidelines rather than a law that is strictly enforced. In the legal review section I will describe both immediate compromises that took place prior to Ford's signing the bill into law and in the subsequent years. The HEW and Church committees represent, perhaps, the height of official state concern with the potential dangers of an emergent state dossier system.

#### THE PRIVACY ACT

The Privacy Act of 1974 (5 U.S.C. § 552a) was designed to protect American citizens from excessive government monitoring and emergence of a centralized, national dossier system. To understand its impact over the subsequent four decades it is useful to focus on two key provisions of the law. The first provision, 552a(b),<sup>17</sup> forbids the disclosure of any records from one agency to another without written request from the subject of the given record, except under certain mitigating circumstances which will be addressed below. A second stipulation of the law, 552a(e)(4), requires that an agency notify the public of any planned new system of records indexed by individual persons and contain personal information by first publishing a "systems of records notice" (SORN) in the *Federal Register*.

---

<sup>17</sup> See relevant U.S. Code at <http://www4.law.cornell.edu/uscode/5/552a.html>.

Restrictions on external disclosure are what Gellman (1997) calls “almost certainly the biggest failure of the Privacy Act.” Acknowledging the impossibility of establishing some fixed statutory test of when disclosure of records was warranted, the authors of the Act left these judgments to the agencies themselves, creating the “biggest loophole in the law.” Perhaps the most significant extenuating circumstance for disclosure is “routine use,” meaning that an agency can disclose a record to another agency if such disclosure is compatible with the original purpose for producing the record:

This vague formula has not created much of a substantive barrier to external disclosure of personal information. Agencies generally operate under the belief that they can disclose any record for almost any purpose if the law’s procedural requirements of publishing a notice in the *Federal Register* is met. Limited oversight of routine use by the OMB and by the Congress had little general effect. (p. 198)

While the notification clause of the Privacy Act has not been without its own problems, one can argue that SORNs have, at times, helped to galvanize resistance to some systems before their deployment. The January, 2003 *Federal Register* notice of the CAPPS II air traveler risk assessment program quickly circulated among privacy NGOs including EPIC, CDT and the EFF, which rallied support among the public and Congress, leading to a congressional bill prohibiting public funding of the program until many critical privacy questions were answered. Subsequent SORNs published to provide details of the successor program, SecureFlight, have also served as rallying points for privacy advocates, leading to a continuing delay and reworking of the program (Bennett, 2008a).

The Privacy Act did address the use of SSNs to some degree and placed new restrictions on their use, but the restrictions were watered down by exemptions. Section 7 of the Privacy Act states:

It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual’s refusal to disclose his social security account number. (Sec. 7(a)(1))

While this would appear to heavily restrict the usage of the SSN by federal, state and local agencies, the clause has been rendered largely irrelevant by a number of important exceptions.

... although this provision applies beyond federal agencies, it does not apply to: (1) any disclosure which is required by federal statute; or (2) any disclosure of a social security number to any federal, state, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

This meant that the IRS, Medicare and Medicaid, the Pentagon and other federal agencies could all continue to use it and require the information before providing benefits. Second, the Tax Act of 1976 exempted all state level agencies “in the administration of any tax, general public assistance, driver’s license, or motor vehicle registration law within its jurisdiction” from the law and stipulated that any other federal law conflicting with this exemption was “null, void, and of no effect” (“Privacy Act Overview,” n.p.).

Further, the Privacy Act contains no restriction on the use of the SSN within the private sector, which grew rapidly in the ensuing decades. Not only does the Privacy Act not cover the private sector, but public sector enforcement has also been weak from the very beginning. Before the Act reached his desk, President Ford warned Sam Ervin of the Senate Judiciary Committee that he would veto the Act unless the proposed Privacy Commission was downgraded from an independent agency to a “Privacy Protection Study group,” with enforcement power relegated to the Office of Management and Budget, an executive branch agency under Ford’s authority. In subsequent administrations, the OMB has done little to enforce the Act in any significant way (Laudon, 1986). For example, Laudon (1986) notes that the Carter and Reagan administrations “sabotaged the ‘routine use’ clause by claiming routine use is any use the agencies say is routine” (p. 375).

In the 27 years following the Privacy Act and before the September 11<sup>th</sup> attacks, protections of the Privacy Act began to erode, while Congress passed a series of sector-specific PII protection laws. One major exception to this rule is the Electronic Privacy Communication Act of 1996.

#### ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA)

While the reasonableness criterion appeared to rescue the Fourth Amendment from its apparent limits to physical, Cartesian space, the steady evolution of electronic information technology has led to its continuing dilution. As technologies with the capacity to monitor individuals in their daily lives increasingly diffuse into the population and become commonly used, the notion of a “reasonable expectation of privacy” changes along with them. As Gandy (1993) notes:

As the technological means to gain or facilitate access to personal information about individuals continue to develop and to become all the more broadly available as the cost, complexity, and skill requirements necessary to use them are all diminished, it will soon be the case that no expectation of privacy at all could be reasonable.(p. 203)

Indeed, as use of the Internet for private communications continues to grow, legal scholars have questioned whether the reasonableness clause can apply at all. The Supreme Court has repeatedly ruled that citizens do not have a reasonable expectation to privacy when their communications are stored by a third party (Kerr, 2004). For example, in the 1976 Supreme Court Case *United States v. Miller*, the court ruled:

[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed. (*United States v Miller*, 425 U.S. 438, 1976, n.p.)

With the Fourth Amendment’s increasingly tenuous ability to protect the privacy of electronic communications, Congress in 1986 passed the Electronic Communications Privacy Act

(ECPA) (P L 99-508, 18 U.S.C. § 2510). The ECPA was passed by the U.S. Congress to explicitly extend legal wiretapping restrictions from telephone to Internet-mediated communications such as e-mail. The ECPA consists of three primary sections, Title I, The Wiretap Act; Title II, the Stored Communications Act; and Title III, The Pen Register Act. The ECPA is an immensely complex body of law written well before the commercial development of the Internet, leading to much confusion over its applicability to online communication both within the courts and the law review literature. It is beyond the scope of this dissertation to review the Act in detail. Instead, we will consider a few of the titles' most important distinctions and the confusion that continues to surround them. The Act distinguishes between communication in transmission and communication in storage, and between envelope (or transaction) communication and content communication.

#### TRANSMISSION V. STORAGE

Whether a particular communication is judged by a court of law to be in transmission or in storage is the most significant determinant of its legal protection. Communication in transmission, that is any communication occurring in real-time, is governed by the Wiretap Act and has the highest legal protection. For the state to intercept real-time communications requires a Title III court order, also known as a super search warrant. Violation of the wiretap act is a felony. Stored communications, on the other hand, is subject to much narrower protection, contains several exceptions, and violation generally constitutes a misdemeanor.

The distinction between stored and transmitted communication on the Internet, however, remains unclear. For example, e-mail, in the course of transmission from sender to receiver, is temporarily stored at multiple intermediate points, sometimes for several days. In a recent case, *United States v. Councilman*, the plaintiff, Brad Interloc corporate executive Brad Councilman, argued that his company's "interception" of email from Amazon to individuals who subscribed to

his company's email service should be governed by the Stored Communications Act instead of the Wiretap Act, since the e-mails were stored on Interloc's servers when they were accessed. Since Interloc was acting as an ISP in this case, they would have been exempted from prosecution under the Stored Communications Act. Although a three judge panel of the Massachusetts First Circuit Court agreed with Councilman, the decision was later reversed in a rehearing by the full First Circuit:

As often happens under close scrutiny, the plain text is not so plain. The statute contains no explicit indication that Congress intended to exclude communications in transient storage from the definition of "electronic communication," and, hence, from the scope of the Wiretap Act. Councilman, without acknowledging it, looks beyond the face of the statute and makes an inferential leap. He infers that Congress intended to exclude communications in transient storage from the definition of "electronic communication," regardless of whether they are in the process of being delivered, simply because it did not include the term "electronic storage" in that definition. This inferential leap is not a plain text reading of the statute. (*United States v Councilman*, vacated en banc, 418 F.3d 67 (1<sup>st</sup> Cir. 2005) (No. 03-1383))

Although the court's decision has largely been interpreted as a victory by privacy advocates, the court neglected to extend protections of the Wiretap act to email communications after they have completed their routing and are stored at their destination server. As a result, there remains a stark difference between legal constraints on surveillance of communication in real-time transmission and communication that has been stored.

#### ENVELOPE VS. CONTENT INFORMATION

As Kerr (2003) has shown, the legal distinction between envelope and content information is maintained across a range of communication technologies. For a piece of traditional postal mail, the content information is sealed away in the envelope, while the envelope information is easily viewable and facilitates its reliable passage from the sender to the receiver. For a telephone call, envelope information consists of the phone numbers of the calling and

receiving parties, and the time and duration of the call, while the content information refers to exactly what was said.

Content information is subject to much higher protection than is envelope information, which is governed by Title III of the ECPA, the Pen Register Act. Whereas the installation of a wiretap that intercepts the content of communications requires a super search warrant and is subject to extensive judicial review, law enforcement agencies can monitor real-time communications for envelope information with the equivalent of a court's rubber stamp. In 1968, when the original pen register act was passed, a pen register was a special device attached to a phone line which recorded the phone numbers of the originating caller and destination. No information about the content of the communication was contained in pen register data, maintaining the distinction between content and envelope information.

### PHASE 3

Noted sociologist David Knoke (2004) defines the September 11<sup>th</sup> attacks as a focusing event, "a rare, sudden and harmful event with high media visibility that draws intense attention to a sociopolitical problem." "If a focusing event so drastically disrupts conventional beliefs and routine practices that it alters fundamental social cognitions about causal relations and perceived risks," Knoke notes, "it may trigger major structural transformations of a policy domain" (pp. 84-5).

Things happened very quickly after 9/11, so it is difficult to explain in a purely chronological narrative. The overall structure of the domestic intelligence and national security apparatus has changed dramatically.

— A major new federal agency, the DHS, has been established to protect the country from natural and made disaster bringing a number of once separate agencies under its authority, including The Federal Emergency Management Agency (FEMA) the U.S.



Coast Guard, the new Travel Security Administration (TSA), and the United States Border Patrol.

— There is a new Director of National Intelligence, who oversees and bridges the once separate intelligence agencies.

— There are a growing number of “fusion-centers,” proto-institutions that serve to bring all state policing capacity, more directly under federal auspices.

— A major new government data initiative has been launched, the *Information Sharing Environment (ISE)*.

#### THE USA PATRIOT ACT

The first major legislation to be passed in response to the 9/11 attacks was “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act” (USA PATRIOT Act) (PL 107-56). Signed into law on October 26, 2001, the Act was rushed through congress without following usual legislative procedure. Most members of Congress did not have time to read it:

Rep. Bobby Scott said, “I think it is appropriate to comment on the process by which the bill is coming to us. This is not the bill that was reported and deliberated on in the Committee on the Judiciary. It came to us late on the floor. No one has really had an opportunity to look at the bill to see what is in it since we have been out of our offices.” Rep. John Conyers, the ranking member of the Judiciary Committee, declared, “we are now debating at this hour of night, with only two copies of the bill that we are being asked to vote on available to Members on this side of the aisle.” (Blumenthal, 2009, n.p.)

The Patriot Act vastly expands the government’s powers to conduct surveillance. Two critical sections of the bill that most dramatically impact the potential configuration of the SDS are section 216, which expands the pen register act and Section 505, which significantly increases the authority of the FBI to demand records from private businesses without judicial oversight.

#### EXPANDING THE PEN REGISTER ACT ENVELOPE VS. CONTENT INFORMATION

In late 2001, the USA Patriot Act explicitly extended the provision of the Pen Register Act to the Internet. Specifically, Section 216 of the Patriot Act, “Modification of Authorities Relating to Use of Pen Registers and Trap and Trace Devices,” added the phrase “routing,

addressing” to the limitations clause of the act, expanding the type of information gatherable by pen register to include email headers and URLs that facilitate the transaction of Internet communication. This expansion of the act has been subject to considerable criticism by privacy advocates such as the Electronic Frontier Foundation, who point out that URLs can be used to retrieve specific documents users might access in the course of an Internet session, or their own communications to a search engine which are often contained in a URL. The Patriot Act modification, however, did not modify the original wording of the clause, which continues to state that pen register devices should be used “so as not to include the contents of any wire or electronic communications.” In the fall of 2005, Judge Collings of the U.S. District Court of Massachusetts partially denied a Justice Department application for routing and address information of four accounts at unnamed service providers, stating:

If, indeed, the government is seeking only IP addresses of the Web sites visited and nothing more, there is no problem. However, because there are a number of Internet service providers, and their receipt of orders authorizing pen registers and trap and trace devices may be somewhat of a new experience, the court is concerned that the providers may not be as in tune to the distinction between ‘dialing, routing, addressing or signaling information’ and ‘content’ as to provide to the government only that to which it is entitled and nothing more. (Collings, 2005, n.p.)

#### NATIONAL SECURITY LETTERS

National Security Letters are an administrative tool used by the FBI to requisition information from private companies when they otherwise might be unwilling to provide it. The FBI was first given authority to use NSLs in 1988 with the passage of the Right to Financial Privacy Act and the Electronic Communications Privacy Act. NSLs at this time, however, were considered to be “narrow exceptions in consumer privacy law, enabling the FBI to review in secret the customer records of suspected foreign agents” (Gellman, 2005, n.p.). Recipients of national security letters, under the original wording of the Patriot Act, were forbidden, in perpetuity, from disclosing the letters to any third party, including legal counsel. Section 505

dramatically expanded the power and scope of NSLs via amendments to the three existing NSL statutes, the ECPA, RFPA, and FCRA. The former requirement that NSLs be directed only at foreign agents or U.S. citizens in communication with foreign agents was removed and replaced with a broader, looser requirement that “the NSL request be relevant to or sought for an investigation to protect against international terrorism or clandestine intelligence activities” (Gorham-Oscilowski & Jaeger, 2008, p.628). The number of FBI agents authorized to make use of the NSL was expanded from a handful of agents at FBI headquarters to more than five dozen supervisors, including special agents in charge of field offices and deputies in New York, Los Angeles and Washington (Gellman, 2005).

The result of the loosening of standards was a major and rapid increase in the number of NSLs filed. In the year prior to the passage of the Patriot Act, only 8500 requests for NSLs were processed. In comparison, more than 143,000 NSLs were issued between 2003 and 2005. According to the FBI IG report, NSL requests often did not meet even the new, looser standards. It found many NSLs were issued without the proper authorization (U.S. DOJ, 2008, March).

Section 505, harkening back to the Church Committee hearings, does specifically state that NSLs powers are granted “provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution of the United States,” but this does not keep innocent Americans from having their PII collected and stored in the process of these investigations.

In 2003, Attorney General Ashcroft rescinded a long-standing Justice Dept guideline which required agents to destroy records gathered on ordinary U.S. citizens when related investigations were closed. Under Ashcroft’s new guidelines, “the FBI shall retain all records it collects and ‘may disseminate’ them freely among federal agencies.” In other words, all

information yielded to the government in the process of pursuing national security letters may now be stored by government databases indefinitely, changing long standing practice in which government agencies expunged data about innocent civilians when particular investigations for which they had been generated came to a close. With President Bush's Executive Order 13388, access to this data was expanded from FBI units to state, local and tribal governments and to "appropriate private sector industries" (Gellman, 2005).

Many new laws have passed since the USA Patriot Act expanding the power of the executive branch to engage in domestic surveillance or otherwise curtail constitutional rights, often without significant public discourse in opposition. On the other hand, specific domestic intelligence initiatives, such as *Total Information Awareness* (TIA), TIPs and TALON (described in the next chapter) have sparked much more directed opposition. Though in many cases public resistance appears to have led to the closure of these programs, in virtually every case, even when "outlawed" by Congress, they continue under new names, often even with the same contractors providing service. In the remainder of this section, I will discuss the TIA initiative, and then look more closely at the 9/11 Commission hearings and their recommendations for institutional restructuring.

#### TOTAL INFORMATION AWARENESS

In November of 2002, investigative reporter John Markoff published a story in the *New York Times* about DARPA's intention to implement a new "system" that would store and analyze virtually all of the information, including most PII, produced within the country's borders and even beyond.

As the director of the effort, Vice Adm. John M. Poindexter, has described the system in Pentagon documents and in speeches, it will provide intelligence analysts and law enforcement officials with instant access to information from Internet mail and calling

records to credit card and banking transactions and travel documents, without a search warrant.

Historically, military and intelligence agencies have not been permitted to spy on Americans without extraordinary legal authorization. But Admiral Poindexter, the former national security adviser in the Reagan administration, has argued that the government needs broad new powers to process, store and mine billions of minute details of electronic life in the United States.

Admiral Poindexter, who has described the plan in public documents and speeches but declined to be interviewed, has said that the government needs to “break down the stovepipes” that separate commercial and government databases, allowing teams of intelligence agency analysts to hunt for hidden patterns of activity with powerful computers. (Markoff, 2002, November 9, n.p.)

Under former felon Poindexter, a new DOD agency was created, the Information Awareness Office (IAO). In version 1.1 of the Total Information Awareness program system description document, the unprecedented scope and breadth of the information gathering program is explained in great detail. In section 3.2.8.3, Human Identification at a Distance (HID), the document makes clear just how important technologies of identification will be within the TIA project:

The goal of the HID program is to develop automated biometric identification technologies to detect, recognize, and identify humans at great distances. These technologies will provide critical early warning support for force protection and homeland defense against terrorist, criminal, and other human-based threats, and will prevent or decrease the success rate of such attacks against DoD operational facilities and installations. Methods for fusing biometric technologies into advanced human identification systems will be developed to enable faster, more accurate and unconstrained identification of humans at significant standoff distances. (U.S. IAO, 2002, July 19, p. 86)

The core focus of the TIA program was that it could analyze, or “data mine” a vast (the total) volume of information so that it could then identify threat patterns. That is, the system, according to its proponents, would be able to detect, for example, a plan to bomb a local mall because of a specific change in buying patterns, communication behavior, or even web browsing.

Although most commentary tended to focus on the concept of a super database, ignoring the equally, if not more chilling plans for ID systems, public reaction to the program was very

negative. Using a former disgraced government official, who had been convicted of multiple felonies for his role in the Iran-Contra scandal, seemed reckless and dismissive of the public interest. The idea that the U.S. government would now watch everything we did and said seemed too out of step with the broad American cultural moral sense of freedom from tyranny. In a November 14, 2002 column, William Safire wrote:

He [Poindexter] is determined to break down the wall between commercial snooping and secret government intrusion. The disgraced admiral dismisses such necessary differentiation as bureaucratic “stovepiping.” And he has been given a \$200 million budget to create computer dossiers on 300 million Americans. (Safire, 2002, November 14, n.p.)

The first DOD response to public reaction was to change the name of the program from *Total Information Awareness* to *Terrorist Information Awareness* and drop the suggestion that new legislation, such as the then in process Homeland Security Act, would be required to authorize the deployment of the program. Instead, the IAO claimed that it would make sure that the system was harmonious with the existing legal environment. The name change and the promise by the IAO to stay within the law, however, were not enough to quell public criticism of the program.

In September 2003, Congress eliminated funding for TIA and dissolved the IAO office in September 2003. The wording of the “conferees’ agreement” on the 2004 defense bill specifically prohibited funding for the TIA project or the transfer of TIA to another agency. *CBS News* wrote, “Pentagon Terror Spy Lab Closed” (Collins, 2003). *USA Today* wrote, “Pentagon’s ‘Terror Information Awareness’ program will end” (“Pentagon’s Terror,” 2003).

The image of the TIA program as Poindexter originally described is what one might call a prototypical state dossier system. The project planned not only to store all available data but be able to reliably identify all human beings at even considerable distances. A superficial view of the U.S. SDS history might lead one to believe that the potential for the U.S. to move into a deeper,

more explicit form of SDS was there in 2002, but responding to public pressure, Congress put the legislative reins on the DOD and successfully ended the threat.

It is important to consider, however, how virtually every aspect of the TIA project, as described, appears to be continuing apace, though under the direction of multiple, at least physically separate institutions. Since the Congressional directive did not specifically address individual components of the program, many if not most or all of these components have in fact been transferred to other agencies. The basic tenets of the TIA program continue, under different names, often with much more subtle wording. As we will see, Total Information Awareness (TIA) has become the Information Sharing Environment (ISE), an initiative with such an innocuous, somnambulant name that it marches on without even the dimmest public awareness. Instead of the TIPS program, we now have the practice of “suspicious activity reports,” a term so generic it is easy to miss.

Investigative reporter Shane Harris (2006) published a lengthy report, based on documents he recovered from TIA contractors, that two key components of the program — the Information Awareness Prototype System, the core database which was to store the entire array of TIA information, and a piece of application software — were renamed to Basketball and Topsail, respectively, and moved to an office under the NSA, Advanced Research and Development Agency (ARDA). Though the responsible agency and names had changed, many of the original TIA contracts were simply maintained.

Two of the most important components of the TIA program were moved to the Advanced Research and Development Activity, housed at NSA headquarters in Fort Meade, Md., documents and sources confirm. One piece was the Information Awareness Prototype System, the core architecture that tied together numerous information extraction, analysis, and dissemination tools developed under TIA. The prototype system included privacy-protection technologies that may have been discontinued or scaled back following the move to ARDA.

A \$19 million contract to build the prototype system was awarded in late 2002 to Hicks & Associates, a consulting firm in Arlington, Va., that is run by former Defense and military officials. Congress's decision to pull TIA's funding in late 2003 "caused a significant amount of uncertainty for all of us about the future of our work," Hicks executive Brian Sharkey wrote in an e-mail to subcontractors at the time. "Fortunately," Sharkey continued, "a new sponsor has come forward that will enable us to continue much of our previous work." Sources confirm that this new sponsor was ARDA. Along with the new sponsor came a new name." We will be describing this new effort as 'Basketball,' "Sharkey wrote, apparently giving no explanation of the name's significance. Another e-mail from a Hicks employee, Marc Swedenburg, reminded the company's staff that "TIA has been terminated and should be referenced in that fashion." (Harris, 2006,n.p.)

#### INSTITUTIONAL RESTRUCTURING

January 27, 2003 the 9/11 Commission convened, gathering data, scheduling hearings, and performing analyses to better understand the institutional, epistemological and cultural conditions which allowed 9/11 to happen. Among its chief recommendations (formally released to the public on July 22<sup>nd</sup>, 2004,) the report calls for a dramatic reorganization of government and breaking down of existing barriers to information sharing:

As presently configured, the national security institutions of the U.S. government are still the institutions constructed to win the Cold War. The United States confronts a very different world today. Instead of facing a few very dangerous adversaries, the United States confronts a number of less visible challenges that surpass the boundaries of traditional nation-states and call for quick, imaginative, and agile responses.

The men and women of the World War II generation rose to the challenges of the 1940s and 1950s. They restructured the government so that it could protect the country. That is now the job of the generation that experienced 9/11. Those attacks showed, emphatically, that ways of doing business rooted in a different era are just not good enough. Americans should not settle for incremental, ad hoc adjustments to a system designed generations ago for a world that no longer exists.

We recommend significant changes in the organization of the government. We know that the quality of the people is more important than the quality of the wiring diagrams. Some of the saddest aspects of the 9/11 story are the outstanding efforts of so many individual officials straining, often without success, against the boundaries of the possible. Good people can overcome bad structures. They should not have to. (9/11 Commission Report, 2004, p. 399)

Structural barriers to performing joint intelligence work. National intelligence is still organized around the collection disciplines of the home agencies, not the joint mission. The importance of integrated, allsource analysis cannot be overstated. Without it, it is not



possible to “connect the dots.” No one component holds all the relevant information. (p. 408)

The commission report did not explicitly call for the establishment of the DHS but did call for a National Counter Terrorism Center (NCTC) to “be a center for joint operational planning and joint intelligence, staffed by personnel from the various agencies” (p. 403). The commission’s broad call for “connecting the dots” and information sharing and its call for the NCTC were answered in the comprehensive, Intelligence Reform and Terrorism Protection Act (IRTPA) of 2004. Not only did the act establish the NCTC and a new Director of National Intelligence to oversee all coordination and analysis of terrorist and subsequent actions upon that data, but it also established a new office of Information Sharing, whose mission could be described as a further rephrasing of the original TIA program.

The federal government, under these new initiatives, increased the role of existing institutions that could share terrorist information. The number of the FBI-led Joint Terrorism Task Forces (JTTFs) grew from 34 in 2001 to more than 100 in 2007 (Johnson, 2004, December 1). New proto-institutions have emerged as well, such as fusion centers and the InfraGard, which will be described in more detail in chapter 4.

#### INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004 (IRTPA)

According to the law’s preamble, the Intelligence Reform and Terrorism Prevention Act of 2004 (PL 108-458) was enacted “[t]o reform the intelligence community and the intelligence and intelligence-related activities of the United States Government, and for other purposes.” IRTPA was sweeping, comprehensive legislation intended to improve coordination between U.S. intelligence agencies and the departments of federal, state and local governments.

As part of the legislation, a new Director of National Intelligence was created to serve as head of the intelligence community, act as the principal adviser to the President, to the National

Security Council and the Homeland Security Council for intelligence matters related to the national security, and oversee and direct the implementation of the National Intelligence Program. A National Counterterrorism Center was established within the office of the DNI, “[t]o serve as the primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism, excepting intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism.”

A key section of the intelligence reform bill (section 1016) is the implementation of an Information Sharing Environment (ISE). According to the text of the law, “The terms ‘information sharing environment’ and ‘ISE’ mean an approach that facilitates the sharing of terrorism and homeland security information, which may include any method determined necessary and appropriate for carrying out this section.”

The President shall... ensure that the ISE provides and facilitates the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies. The President shall, to the greatest extent practicable, ensure that the ISE provides the functional equivalent of, or otherwise supports, a decentralized, distributed, and coordinated environment that-

- (A) connects existing systems, where appropriate, provides no single points of failure, and allows users to share information among agencies, between levels of government, and, as appropriate, with the private sector;
- (B) ensures direct and continuous online electronic access to information;
- (C) facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations and operations;
- (D) builds upon existing systems capabilities currently in use across the Government;
- (E) employs an information access management approach that controls access to data rather than just systems and networks, without sacrificing security;
- (F) facilitates the sharing of information at and across all levels of security;

(G) provides directory services, or the functional equivalent, for locating people and information;

(H) incorporates protections for individuals' privacy and civil liberties; and

(I) incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls.

The ISE initiative is critical to understanding the ongoing development of the SDS in the U.S.. Programs which fit under its rubric, including fusion centers, suspicious activity reporting and InfraGard are discussed in detail in chapter 4.

Sections 7208-7220 of the IRTPA lay the legal foundation for the establishment of a national, biometric identity card system and allow the federal government to set minimum standards for birth certificates, driver's licenses and other forms of state issued identification. The law directs the Secretary of Homeland Security to establish new standards for ID for domestic air travelers. Although IRTPA is now the basis on which the federal government claims the authority to issue ID standards, the specifics of these standards were left to subsequent legislation such as the Real ID Act.

Section 4012 and Sections 7201-7220 provide the legal basis for an "advanced airline passenger screening system" that "will allow the Department of Homeland Security to assume the performance of comparing passenger information, as defined by the Assistant Secretary, to the automatic selectee and no fly lists, utilizing all appropriate records in the consolidated and integrated terrorist watchlist maintained by the Federal Government." The system proposed in the law, which would become known as the "Secure Flight" system, was the third attempt by the federal government to assess travelers for their potential risk without running afoul of general civil rights protections.

## RECENT CHALLENGES TO NSLS

The issue of national security letters raised and continues to raise profound questions. Two court cases, *Doe v Ashcroft* and *Doe v Gonzalez*, challenged the FBI's use of NSLs on constitutional grounds.

In *Doe v Ashcroft*, an internet service provider sued the government after receiving an NSL, arguing that section 2709 of the ECPA, as amended by the Patriot Act, violated both its First and Fourth Amendment Rights. The plaintiff argued that the law “gives the FBI extraordinary and unchecked power to obtain private information without any form of judicial process” and that the NSL gag order “burdens speech categorically and perpetually, without any case by-case judicial consideration of whether the speech burden is justified.”<sup>18</sup> A similar argument was made in *Doe v Gonzalez*, although First Amendment issues were emphasized. The plaintiff argued that the NSL gag order forbid the librarian who received the NSL from taking part in the then ongoing debate on the Reauthorization of the Patriot Act. In both cases, the courts found in favor of the plaintiffs, finding that “the NSL statutes could not withstand constitutional scrutiny unless more explicit provisions were made for judicial review and permissible disclosure by recipients” (U.S. CRS, 2007, March 20, p. 8).

Partially in response to the court's findings, Congress modified section 505 of the USA Patriot Act in the Reauthorization 2005. Section 115 of the Reauthorization Act gives the recipient of an NSL the power to petition the U.S. District court to modify or set aside the request. “The court may modify or set aside the request if compliance would be unreasonable, oppressive, or otherwise unlawful.” The Reauthorization also modified the non-disclosure provision. Under section 116 of the Reauthorization, disclosure of the receipt of an NSL is now no longer automatically attached to the NSL. Rather, disclosure is prohibited upon certification

---

<sup>18</sup> 334 F. Supp. 2d 471 (S.D.N.Y. 2004)

that doing so “may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.” Even if the recipient is compelled to non-disclosure, they still have the right to communicate with “any person whose assistance is needed to comply with the NSL request or to an attorney to obtain legal advice or legal assistance concerning the NSL.”

Following these changes to the law, the U.S. government appealed the lower court findings of the two NSL Court cases to the Second Circuit in *Doe I et al. v. Gonzalez*. The Second Circuit found that the changes to the Patriot Act in the Reauthorization eliminated the constitutional shortcomings that had been highlighted in the original cases.

At the outset of its opinion, the court observed that one of the effects of the Reauthorization Act was to “dramatically alter § 2709 [of the ECPA].” The appeals court vacated the Fourth Amendment portion of the district court’s opinion in Ashcroft because the addition of “provisions permitting NSL recipients to challenge the issuance of NSLs in court” rendered that portion of the appeal moot. As to the First Amendment issues, the appellate court determined that the lower court was in a better position to address those issues in the context of revised Section 2709 and therefore remanded that portion of the case. With respect to the Gonzalez case, the Second Circuit held that, inasmuch as the government consented to the disclosure of the NSL recipient’s identity, the appeal was rendered moot by the government’s voluntary actions and the case was dismissed (449 F.3d 415, 2006, n.p.).

Despite the changes to the law, numerous concerns about NSLs remain. Although there is now opportunity for recipients to engage the judicial system if they feel the NSL is unwarranted, the broad conditions under which the FBI may issue an NSL remain. Further, judicial review does not occur before the NSL is issued but only after, and only if the recipient chooses to engage the court. Further, the court must take the government’s representation that a nondisclosure order is

necessary on faith. The court “has no authority to actually weigh factors in determining whether a gag is appropriate.”<sup>19</sup>

## E-GOVERNMENT ACT

The E-Government Act (PL 107-347, 44 U.S.C. § 101), passed in 2002, is a law “[t]o enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services, and for other purposes.” Included within the 72 page act is a provision requiring that any government agency, before “developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form” or beginning a new collection of identifiable information that will be “collected, maintained, or disseminated using information technology” that affords the “physical or online contacting” of ten or more individuals not under government employment, must first conduct a “privacy impact assessment” (PIA). The PIA must address the following seven issues:

- (I) what information is to be collected;
- (II) why the information is being collected;
- (III) the intended use of the agency of the information;
- (IV) with whom the information will be shared;
- (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
- (VI) how the information will be secured; and
- (VII) whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the “Privacy Act”).

---

<sup>19</sup> *Use of National Security Letters: Hearing before the Subcomm. on the Constitution of the Senate Comm. on the Judiciary*, 110th Cong. (April 11, 2007) (statement of Bob Barr, Chief Executive Officer, Liberty Strategies, Inc.)

The reporting requirements under the E-Government Act are broader than the SORN in the Privacy Act. While the Privacy Act is limited to a system of records, any IT system that contains PII, whether it is designed specifically to retrieve information based on individual entities, must have a privacy impact assessment. However, it is important to note that the E-Government Act allows exceptions to this rule; it “may be modified or waved for security reasons.” It should be stressed, as a result, there may be IT systems developed by the federal government which contain personally identifiable information but, for security reasons, are not reported to the public. Nevertheless, as we will see, PIAs offer an important window into the current state of the U.S. SDS.

#### FTC AND DHS ARTICULATIONS OF THE FAIR INFORMATION PRACTICES (FIPS)

Today, the most relevant codifications of the FIPs (originally articulated by the HEW Committee) are those of the FTC, directed at the private sector, and the DHS. It is important to remember that, unless otherwise encoded in law, these principles have only the strength of guidelines or model codes. Any activities involving the collection and use of PII by the DHS, if related to national security, are already exempt from the Privacy Act, meaning that compliance for a particular program lies within agency discretion and is ultimately not subject to independent oversight. It is useful to consider these articulations in some detail, as they represent the most direct codification of principles for dealing with PII in the public and private sectors today.

#### FTC RE-ARTICULATION OF FAIR INFORMATION PRACTICES

Common to all of these documents (hereinafter referred to as “fair information practice codes”) are five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.

#### Notice

The most fundamental principle is notice. Consumers should be given notice of an entity's information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information.<sup>(29)</sup> Moreover, three of the other principles ... are only meaningful when a consumer has notice of an entity's policies, and his or her rights with respect thereto.

### Choice

At its simplest, choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information — i.e., uses beyond those necessary to complete the contemplated transaction. Such secondary uses can be internal, such as placing the consumer on the collecting company's mailing list in order to market additional products or promotions, or external, such as the transfer of information to third parties.

### Access

Access refers to an individual's ability both to access data about him or herself — i.e., to view the data in an entity's files — and to contest that data's accuracy and completeness.

### Integrity

To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form.

### Enforcement

It is generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them. Absent an enforcement and redress mechanism, a fair information practice code is merely suggestive rather than prescriptive, and does not ensure compliance with core fair information practice principles. Among the alternative enforcement approaches are industry self-regulation; legislation that would create private remedies for consumers; and/or regulatory schemes enforceable through civil and criminal sanctions.<sup>20</sup>

## DEPARTMENT OF HOMELAND SECURITY POLICY

The Department of Homeland Security's Privacy Office also refers to the FIPs and the role of the Privacy Act, but articulates them in a different, more extended form than the FTC.

The FIPPs form the basis of the Department's privacy compliance policies and procedures governing the use of personally identifiable information (PII). These principles are: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability

---

<sup>20</sup> Retrieved 7/20/2009 from <http://www.ftc.gov/reports/privacy3/fairinfo.shtml>



and Auditing. DHS uses the FIPPs to assess and enhance privacy protections by analyzing the nature and purpose of the collection of PII to fulfill DHS's mission and how the Department can best provide privacy protections in light of these principles.

Again, while these principles continue to be articulated in contemporary policy statements, they are best thought of as guidelines and best practices rather than laws.

## CHAPTER 4: U.S. CASE

This chapter examines the current state of the U.S. dossier system in terms of the two primary components of the general model: *ID systems* and *systems of records*. The ID systems section first provides a brief historical overview of state driver's licenses and the social security system before analyzing the federal government's case and the public's reaction to a set of national standards for state-issued driver's licenses: the Real ID initiative. The systems of records section, divided into three sub-sections, considers U.S. record systems at two levels of analysis: 1) record systems as wholes and 2) types of records. At the record system level, I consider the FBI's *Investigative Data Warehouse* (IDW), a record system that, according to the FBI's 2004 report to the 9/11 Commission, is designed to contain all the data that can be legally stored in one place. At the level of individual record types, I consider the emergence of *suspicious activity reports* (SARs) and *watch lists*. SARs are nationally standardized records of suspicious activity that often contain PII. Watch lists are an increasingly important tool of the state dossier system that reduces potentially voluminous dossier data to a binary decision (*on* or *off* the list). As we will see, watch lists enable state agents to act on dossier subjects in a manner that lies largely outside judicial review.<sup>21</sup>

### ID SYSTEMS

As will become very clear in the course of this section, it can be difficult to define, definitively, what constitutes a national ID system. A number of scholars have argued that the use of driver's licenses to prove identity and the widespread public and private use of the social security number to index personal records means that the U.S. had a *de facto* national ID system already in place even prior to the passage of the Real ID Act (Eaton, 1986; Sobel, 2002;

---

<sup>21</sup> For research notes concerning how I arrived at these particular case nodes, please consult *Appendix A*.

Froomkin, 2004). The National Research Council uses the term “nationwide identity system” to describe any large-scale system, without restricting them to formal “national identity systems” (Kent & Millet, 2003, p. 3). Legal scholar Richard Sobel (2002) has coined the term National Identification System (NIDS) to refer to a “system of national ID numbers, databanks and identity cards.” Although Sobel intends the term to cover the collectivity of U.S. SoRs containing PII and ID systems such as social security, the term also suggests a narrower interpretation, to refer specifically to the ID systems and their supporting databases.

While critics of the current Real ID initiative are largely in agreement that the program is a national ID, the U.S. government has maintained that it is only a flexible set of standards. The U.S. further argues that Real ID will lower the risk of a domestic terror attack while simultaneously reducing identity theft. Public resistance has been strong however, and it appears that the Real ID program is losing momentum. Nevertheless, careful examination of the struggle over Real ID reveals a different picture, one where public resistance to particular components of a national ID system, such as the use of RFID to track human beings, has been largely ineffective. This section will, first, provide some historical context on U.S. state driver’s licenses and the social security number system before focusing on the U.S. government’s call for and justification of the Real ID, public reaction to the initiative, and the state of Real ID as of summer, 2009.

#### HISTORICAL BACKGROUND: DRIVER’S LICENSE AND ID

Although it is often assumed that driver’s licenses were introduced to make the roads safer, most of the initial state programs were strictly revenue generators, without any form of test required, only the filling out of a form and the payment of a fee (Watner, 2004). According to the American Association of Motor Vehicle Administrators, Massachusetts, in 1907, was the first state to issue a driver’s license. By 1978, there were more than 140 million driver’s licenses in the U.S. nationwide. Over the past several decades, the driver’s license has become the favored proof

of identity for commercial transactions that require identity or for general proof of age. Its role as general proof of identity has become so significant that by 1977 at least 40 states were issuing “non-driver’s licenses” for those who did not drive but needed a state-issued identity document for other purposes.

State laws require drivers on public roads to carry their licenses at all times. Partially as a result of this legal requirement and its role as a general identifier for commercial transactions, the license has become ubiquitous in U.S. resident’s wallets and pocket books. State driver’s license programs have been traditionally outside of federal control, making them poor candidates, in and of themselves, to play the role of a formal national ID card. More recently, beginning with the Immigration Reform Act of 1996 and culminating with the Real ID Act of 2005, the U.S. government has been attempting to assume greater authority over the issuing of driver’s licenses. I will discuss this in detail after providing a brief history of the social security card and number system.

In August of 1935, President Roosevelt signed into law the Social Security Act (P.L. 74-271). The social security number was not designed to be a general purpose identifier for public and private institutions but rather an index for a specific system of records managing the provision of pensions. The act established a federally regulated pension system for Americans that involved deducting money in the form of a tax on worker’s paychecks, depositing the money in Washington, and then paying money back to the workers in the form of a monthly check after retirement. In order to establish the system, the government, for the first time, began to collect and store personally identifying information that would be used to determine benefits as individuals became eligible. Although the government had collected personal information from the majority of the public before in the ten year census, this marked the first time that personal

information would be collected by the federal government for anything other than statistical purposes (Smith, 2004).

Many recent European immigrants, who had experienced authoritarian governments where papers had to be produced upon demand, were wary of the dangers of a national ID system. Newspaper editorials also weighed in about their concerns that the system would become a national database containing detailed information on all American citizens:

The *Boston American* wrote, “Your personal life will be laid bare, your religion and the church you attend will be listed. Your physical defects will go down in black and white... your union affiliation will be stated.... Even your divorce, if you have one, will be included.” (Smith, 2004, p. 205)

In order to get public support for the act, the Roosevelt administration was careful to frame social security as a limited program focused solely on the provision of pension benefits to the public. Promotional literature spoke of the “assigning” of social security numbers to adult workers. The word “registration” was never used to avoid connotations of regimentation. The Post Office was chosen as the venue for filling out social security applications, as surveys showed that American citizens trusted it much more than other government agencies (Smith, 2004). The PR campaign was highly successful. Between November 1936 and June 1937 more than 30 million applications for SSNs were processed by the Social Security Board (U.S. Social Security Administration, n.d.).

While the concerns raised by newspaper editorials like the *Boston American* were factually inaccurate at the time (applicants needed only to provide their name, birth date and parents’ names, and the social security file itself stored only earnings information) they turned out to be quite prescient. Over the next several decades, the uses of the SSN and the range of data indexed to it, increased dramatically.

Although the Social Security Board had pledged that social security data would remain confidential even in the face of a subpoena, a 1939 executive order by Roosevelt gave the FBI access to social security files in the course of criminal investigations. More significantly, Roosevelt's 1943 Executive Order 9397<sup>22</sup> required all federal agencies to use the SSN as the personal identifier for any new "system of accounts." While not significant at the time given the low state of database technology, the order set the stage for an explosion in use of the SSN in the 60s and beyond.

In 1961, SSNs were required as taxpayer IDs for the filing of federal taxes; state tax bureaus soon followed suit. In April 1964, the Commissioner of Social Security approved the use of SSNs for students in 9<sup>th</sup> grade or above (U.S. HEW, 1973). In July 1969, the U.S. DOD stopped issuing serial numbers to troops and adopted social security numbers in their place. The DOD said the new policy would fall in line with Roosevelt's 1943 Executive Order and increase efficiency in personnel record keeping (Lear & Reynolds, 2003). By the end of the 60s, social security numbers were being used to index personal information records for Medicaid, Medicare, and the Veteran's Administration as well (U.S. HEW, 1973).

In 1970, a new banking law required banks to record social security numbers of their customers, opening the floodgates to private industry use of the SSN that would extend first to insurance companies and then beyond to include most any form of business from cable television to magazine subscriptions. In 1973, the U.S. Department of Transportation was using the SSN to index and retrieve records in its "National Driver Register," although it could not yet require their use (HEW, 1973). This changed (albeit only temporarily) twenty three years later, with the passing of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996. Section 656(b) of the Act stated that federal agencies could not accept for identification purposes a

---

<sup>22</sup> Exec. Order No. 9397, 3 C.F.R. 283-84 (1943-48) ordering federal agencies to use the social security number, available at [http://www.defenselink.mil/privacy/pdffdocs/EO\\_9397.pdf](http://www.defenselink.mil/privacy/pdffdocs/EO_9397.pdf), retrieved May 19, 2009.

driver's license or compatible document that did not meet specific requirements including: "a social security account number that can be read visually or by electronic means" (Twight, 2004, p. 154). States were now required to collect and display the SSN for all applicants for a range of state licenses, from fishing licenses to marriage licenses, to, most importantly, driver's licenses. Buried within the much larger Welfare Reform Act, these two requirements together essentially implemented a national ID card indexed to the social security number.

States could opt out of the initiative at the cost of losing federal funding. Unnoticed within this larger bill, public resistance to the SSN provisions did not stir until 1998, when states began attempting to implement the new regulations. In 1999, the statute was repealed (Smith, 2004; Smith, 2006). Today, the practice of putting a social security number on a driver's license is largely agreed to put the subject at significant personal risk; it is unlikely to be seriously proposed in legislation again. Congress revisited and reasserted the federal government's power to dictate standards for driver's licenses, however, in IRTPA (2004) and the Real ID Act of 2005.

Also in 1996, Congress passed the "Personal Responsibility and Work Opportunity Reconciliation Act of 1996" (PL 104-193). Often referred to as the "deadbeat dad" law, the legislation called for the implementation of a new system of records, the Federal New Hires Database, designed to identify, locate, and force payment from divorced fathers attempting to avoid child support. Under the law, every employer in the country is mandated to provide the name, address, and social security number of all new employees to state officials. The states must then give this information, along with wage and unemployment information, to the federal government for inclusion in the database (Twight, 2004; Smith, 2004).

When the first social security cards were issued, infants and school age children were not issued cards because, logically, they were not working age and could not receive the benefits the

system was designed for. Today, most infants are issued social security cards within weeks of their birth, as part of a federally funded initiative:

To facilitate the assignment of SSNs at birth, the federal government has financed state programs to secure issuance of the numbers as part of the birth-certificate registration process, an enticement that has enabled the Social Security Administration to secure adoption of its “Enumeration at Birth” process in all fifty states” (Twight, 2004, p. 153).

Although the Social Security card itself was explicitly labeled “not for identification,” the social security number has clearly assumed this role. Criminals, armed with the numbers of unsuspecting victims, were able to open up credit cards and other accounts in their name, beginning the scourge of “identity theft” which rose to epic proportions in the 1990s.

Of all the pieces of information to be gained, SSNs are the holy grail of identity thieves. With these numbers, one can potentially access all of the databases that use SSNs as primary database keys. Where pre-cyberspace thugs concerned themselves only with the cash and credit cards in a wallet, thereby limiting the “take” to the sum of the cash and that part of the credit limit that could be captured before the cards were cancelled, the bounty of the identity thief is the person’s entire credit worthiness-their ability to buy homes, cars, and obtain educational loans. Everything! In urban areas, identity theft rings eagerly pay a premium for stolen wallets that contain SSNs and other identifying data; stolen credit cards can be left for the street urchins. (Berghel, 2000, p. 20)

As the growth in Internet use in the U.S. has contributed to the frequency of identity theft, government policy toward the use of SSNs has begun to swing in the other direction. A task force commissioned by President Bush to study identity theft, in its September 16, 2006 interim report, recommended that the government “limit the unnecessary use in the public sector of Social Security numbers (SSNs), the most valuable consumer information for identity thieves” (U.S. FTC, 2006, September 16, p. 1). As part of this, the task force recommended:

The Office of Personnel Management (OPM), in conjunction with other agencies, should accelerate its review of the use of SSNs in its collection of human resource data from agencies and on OPM-issued papers and electronic forms, and take steps to eliminate, restrict, or conceal their use (including the assignment of employee identification numbers, where practicable) ( p.1).



Although the task force recommendation is a step forward, most federal agencies that already use SSNs continue to use them and there are still no restrictions on the use of SSNs by private businesses. Citizens have the right to refuse to submit their SSNs when demanded by business, but the business has the right to refuse service if the number is not provided. It does appear unlikely, however, that any future ID card initiative could now make a case for using the SSN as the unique ID number displayed on the card. The debate and ongoing struggle over the Real ID initiative is not focused on the issue of a unique number, but other physical aspects of the card, its intended uses, and the federally standardized process for issuing the card securely.

#### THE REAL ID PROGRAM: KEEP TERRORISTS OFF THE PLANES

Good morning, everybody. One of the first and most important priorities at the Department of Homeland Security is to protect America from individuals who are trying to do us harm. When we investigated the infamous attacks of September 11, 2001, one of the things that we discovered was that 18 of the 19 perpetrators had been issued U.S. identification documents, including state driver's licenses, and that some of these documents had been obtained fraudulently.

Two of the hijackers, Hani Hanjour and Khalid al-Mihdhar obtained the paperwork for their Virginia driver's licenses by handing \$100 to an illegal alien in a convenience store parking lot. And then, that alien signed the forms attesting that these two hijackers were local residents. And, it was that fake ID, those phony driver's licenses that enabled these hijackers and others to rent cars, board planes, and otherwise take the steps they needed to carry out their murderous plans. ("DHS: Remarks by Secretary Chertoff," 2007, n.p.)

As Chertoff argues here, if the government can make it hard for terrorists to obtain fraudulent ID cards it will become much more difficult for them to infiltrate and endanger the homeland. This argument is made in more formal terms in the March 2007 "Real ID Notice of Proposed Rulemaking (NPRM):"

In summary, if these requirements lowered by 3.60% per year the annual probability of a terrorist attack that caused immediate impacts of \$63.9 billion (which is an estimate of the immediate impact incurred in the 9/11 attack and might be considered a lower bound estimate), the quantified net benefits of the REAL ID regulation would be positive. If these requirements lowered by 0.61% per year the annual probability of a terrorist attack that caused both immediate and longer run impacts of \$374.7 billion (which is an estimate of the immediate and longer run impacts incurred in the 9/11 attack and might

be considered an upper bound estimate), the quantified net benefits of the REAL ID regulation would be positive. (72 FR 10820, 2007, p. 10846)

In addition to its argument about reducing terrorism, the government claims other likely benefits for the program including the reduction of identity theft, fraudulent access to government subsidy and welfare programs, voter fraud, unlawful employment and unlawful access to firearms. Government claims about the improved security of Real IDs have been widely challenged by academics and other experts (Lemos, 2006; Vijayan, 2007; Schneier, 2007b; Perrin, 2009). While it is agreed that tougher issuing standards could make it difficult for terrorists and criminals to fraudulently obtain driver's licenses, no system is completely immune to outsider hacking and insider corruption. Further, tougher standards for the ID simultaneously increase the value of cracking the system, making any advances in security temporary at best. The value also grows as more record systems become networked together to support the identification and registration process:

This is, of course, a fundamental problem inherent in the very nature of any massive, centralized government data-sharing plan that spans multiple agencies and connects untold numbers of state and federal law enforcement officers: the usefulness of such a system to any one individual (a white hat or a black hat) grows roughly with the square of the number of participants who are using it to share data (Metcalf's law). So the more white hats that any of these programs manage to connect to each other, the more useful the network as a whole will be to the small handful of black hats who gain access to it at any point. (Stokes, 2009, n.p.)

The Real ID Act of 2005, sponsored by House Judiciary Committee chairman James Sensenbrenner (R-Wisconsin), was passed as a rider to a critical military spending bill, Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005 (HR 1268). The bill became mired in committee and could not advance on its own. This lack of public support has marked its every step, from its initial passage, to the proposed Real ID rules released in March, 2007 and the final rules released on January 11<sup>th</sup>, 2008.

In the wake of the Act's initial passage, with public sentiment aligning against the program, the DHS engaged in a PR program to convince the public that they were not, in fact, implementing a national ID.

Critics of REAL ID often misrepresent what it is and what it is not. Probably the most egregious myth is the claim that the law creates a national ID that Americans will be required to carry.

Wrong. REAL ID is simple. The regulation requires that states meet minimum security standards when they issue driver's licenses and identification cards necessary for "official purposes," like getting on a plane or entering federal buildings. That's it. The federal government's role is to make sure that states meet minimum standards of security, so that banks and airports in one state can count on the quality of licenses issued in another. (Baker, 2008, n.p.)

#### SUPPORT OF PRIVATE INDUSTRY

In addition to the strong backing of the U.S. federal government, the Real ID initiative has the support of private industry, in particular those in information technology and security such as the Security Industry Association (Pero, 2002), the Smart Card Alliance, and the Information Technology Association of America (ITAA), which includes companies such as Microsoft, Yahoo, and Verizon. In September 2007, the ITAA wrote to the U.S. Congress to request that \$50 million dollars be appropriated for Real ID:

Dear Chairman Byrd and Ranking Member Cochran:

On behalf of our more than 300 member companies and the information technology industry at large, the Information Technology Association of America (ITAA) respectfully urges the Senate to recognize that the federal government must share in the financial burden of implementing the Real ID Act by ensuring the \$50 million in grant funding remains in the FY '08 Department of Homeland Security (DHS) Appropriations bill. These sorely needed funds will allow the states to begin overhauling the driver's license and identification systems that have been linked to the terrorist attacks of September 11, 2001, thousands of identity thefts each year, and many other crimes.

In the letter, ITAA cites a survey that they purport shows overwhelming public support for Real ID. The survey, sponsored by the ITAA and conducted by "Public Opinion Strategies," asked the respondents to agree or disagree with the statement "[s]tates should be required to meet national

minimum standards for driver's licenses and IDs to make it harder for criminals to use fake IDs to commit crimes, such as identity theft." 91% per cent of respondents agreed.

As Gandy (2003) reminds us, however "the fact that a particular question is asked may add legitimacy to a policy option that might otherwise not be considered" (p. 284). Another 2007 survey, conducted by the ACLU in the same year, paints a different picture of public sentiment. The survey asked: "[i]n order to help the government fight terrorism, each state would establish new driver's licenses that will record your personal information in a database and share it with other states and the federal government." 46% opposed or strongly opposed.

The ITAA letter helps make clear the interest of multinational corporations in the expansion of government supported ID systems. The size of the U.S. Homeland Security market has been growing at a high rate, expected to continue to more than triple over a five year period. \$7 billion dollars in 2001, the homeland security market totaled 46.2 billion in 2005. In 1999, only nine private firms were receiving homeland security contracts. In 2003, 3,512 companies were receiving contracts. In 2005, this number had ballooned to 33,890. Lobbying firms also began to increasingly specialize in homeland security. By the end of 2005, 543 companies, individuals and lobbying firms had registered as homeland security lobbyists, up from just two in 2001. Homeland Security Research Corporation predicts that the market will be worth \$178 billion by 2015, tripling in size twice over a ten year period. Among the business opportunities within this market, according to Imperial Capital, are border and perimeter security, biometrics and credentialing, records management and data mining, and scanning devices.

#### RESISTANCE TO REAL ID: FINANCIAL COST AND HUMAN RIGHTS

Given the disagreement over just what constitutes a "national ID system," I will not focus on this binary condition (*is/isn't* a national ID system). Details related to this dispute, however,

are worth considering for other reasons, as they help us to identify key components of a national ID system, as well as their potential life outside and endurance beyond specific, named programs like Real ID. To see this struggle in its broader context, I will first consider resistance to the Real ID as a specific program. The policy as a whole, including the three individual aspects that I have already identified above, was resisted by the individual states for two primary reasons: *cost* and *human rights*. While the issue of cost has probably been the major determining factor in the Real ID's apparent demise, human rights issues have been raised by many states and many U.S.-based NGOs. Combined, these two dimensions did seem likely to derail Real ID as of mid 2009, but again, not significantly slow down the U.S.'s march to an increasingly comprehensive national ID system.

In September, 2006, the National Governors Association estimated that the total cost to implement Real ID would exceed \$11 billion, with an initial upfront cost of \$1 billion, followed by ongoing costs of more than \$10 billion during the first five year period. This initial estimate, which was based solely on the Real ID Act itself and not subsequent rulemaking, projected that re-enrollment costs (getting the state's entire population of adult drivers back into DMV offices to reapply), would make up the bulk (\$8.48 billion) of this ongoing cost ("The Real ID Act: National Impact Analysis," 2006). The DHS followed in March, 2007 with its own estimate of 23 billion dollars (72 FR 10820, 2007, p. 10845), noting that it could see no way to avoid the high costs of 813 million projected issuances of Real ID over ten years. In a May 1<sup>st</sup>, 2007 letter to DHS Chairman Michael Chertoff, the AAMVA commends the DHS for offering "more realistic" cost estimates, but calls for federal funding:

The fiscal year 2006 Budget included \$40 million, of which only \$6 million has been allocated for "state pilot" projects. The fiscal year 2007 Budget includes zero funding for states or DHS. Funding must be secured that is reliable and ongoing for the states and DHS. We understand that the fiscal year 2008 Budget also includes no funding for REAL ID. AAMVA members encourage DHS to seek and secure funding for fiscal year 2009,

especially for the states to begin implementation of REAL ID. The short term success of REAL ID requires federal funding and the long term success will require ongoing annual, federal appropriations. (Calvin, 2007, p. 6)

DHS responded to these cost concerns in the Real ID final rules with a dramatically scaled back timeline for issuing Real IDs for current driver's license holders and otherwise loosened program requirements. This reduced the estimated cost of implementation from 22 to just over \$3 billion. Nevertheless, the states have continued to register their dissatisfaction with the unfunded federal mandate:

Governors, state legislators and motor vehicle administrators are pleased that many of the regulations seem to reflect comments and recommendations submitted by the three groups to DHS, including extending compliance deadlines and giving states flexibility to manage their systems and make them more secure. DHS also recognized that the implementation cost was an issue by making changes to reduce costs to states. Their estimate remains significant at \$3.9 billion. To date, however, Congress has appropriated less than 3 percent of the projected costs to assist states. ("State Groups Acknowledge," 2008, n.p.)

Concerns about the human rights and privacy implications of the Real ID card have been widespread, with objections on this basis running the gamut from conservative Christian groups like Eagle Forum and more "liberal" groups such as the ACLU. To these groups, there is little question that the Real ID initiative is in fact a national ID program. The Electronic Frontier Foundation (EFF), quoted below, offers a typical human rights criticism of Real ID:

Once the IDs and database are in place, their uses will inevitably expand to facilitate a wide range of surveillance activities. Remember, the Social Security number started innocuously enough, but it has become a prerequisite for a host of government services and been co-opted by private companies to create massive databases of personal information. A national ID poses similar dangers; for example, because "common machine-readable technology" will be required on every ID, the government and businesses will be able to easily read your private information off the cards in myriad contexts. ("Real ID: Threatening Your Privacy," n.d.)

Although human rights and privacy concerns took a back seat to cost issues with the major state associations like the NGA, there was considerable concern raised at the individual

state level. The 2007 State of New Hampshire law outlawing Real ID was an impassioned call to respect human rights and honor the Constitution:

The general court finds that the public policy established by Congress in the Real ID Act of 2005, Public Law 109-13, is contrary and repugnant to Articles 1 through 10 of the New Hampshire constitution as well as Amendments 4 through 10 of the Constitution for the United States of America. Therefore, the state of New Hampshire shall not participate in any driver's license program pursuant to the Real ID Act of 2005 or in any national identification card system that may follow there from.<sup>23</sup>

While human rights concerns have been effectively articulated at the state and NGO level, in public awareness programs and in congressional testimony, resistance to the Real ID program could not have gained traction without overriding concerns about cost.

#### VICTORY?

As of August, 2007, more than 17 states had passed legislation rejecting the Real ID mandate (Lipowicz, 2007b). When the initial, May, 2008 deadline for Real ID compliance had passed, no states were implementing Real ID. As of May, 2009, many states appeared ready to defy federal threats that citizens from states without Real ID would not be able to board airplanes or enter federal facilities after the December 31, 2009 deadline. Further, the governor of one of the states to outlaw Real ID, Janet Napolitano of Arizona, became U.S. Attorney General in early 2009 as part of Obama's presidential administration. Given this fact, it seemed less and likely that states which refused to implement the Real ID initiative would be met with any significant penalty.

This led many to declare the Real ID program officially dead. In an October 2008 article in *Reason* magazine, author David Weigel asks "Who Killed Real ID?"

Deride them all you want, but the nuts are winning real victories for liberty, assembling a ragtag coalition that has managed to beat back one of the most egregious recent assaults

---

<sup>23</sup> New Hampshire, HB 685, 2007 session, approved/effective June 27, retrieved 7/20/09 from <http://www.gencourt.state.nh.us/legislation/2007/hb0685.html>.

on individual privacy. “I think Real ID is done in Arizona,” says Mary Lunetta, an American Civil Liberties Union (ACLU) liaison who worked with Johnson on HB 2677. “It’s over.” Michael Hough, a coordinator for the conservative American Legislative Exchange Council, thinks Real ID will meet a similar fate at the federal level. “Even the administration has backed off of implementing Real ID,” Hough says. “It’s not going to happen as it stands now.”

The left/right, mainstream/fringe hydra of a movement to defeat Real ID in Arizona is a template that has worked in state after state. These strange, sweet victories are a sign that the United States is rediscovering its civil libertarian roots after the momentous disruption of 9/11. (Weigel, 2008, n.p.)

As the passage above makes clear, it is possible to look at the evolution of federal government requirements for Real ID into the final rules and claim that anti- Real ID activists won an important victory for privacy. While this may be true in the obvious sense, that the Real ID initiative may very well die a slow death because of public resistance, it is much harder to argue that this has resulted in any kind of setback to the evolution and expansion of ID and dossier systems. We can see this more clearly by breaking down the Real ID system, not into the two major logics of resistance (cost and human rights), but into its key aspects and components.

The Real ID Act more specifically articulated requirements based on authority that the federal government assumed in 2004, under the IRTPA.<sup>24</sup> The Act identifies three aspects of ID systems — *initial card issuance*, *card use*, and *card specifications* — that will outlast any individual system/project like Real ID, and that help us to more clearly understand the nature and progression of the struggle over ID systems within the context of the SDS. Each of these components were expressed in increasing detail from the initial text of the Act (PL 109-13) to the first Notice of Proposed Rulemaking (NPRM) (72 FR 10820) and finally with the final rules in January 2008 (73 FR 5271).

---

<sup>24</sup> As I discuss above, the federal government had assumed this authority under the 1996 Illegal Immigration Act, but Congress rescinded this power in 1999.



### 1) INITIAL CARD ISSUANCE

One of the primary arguments for the Real ID program has been that many states need to have better protocols for identifying prospective driver's license holders. Without careful authentication of so-called breeder documents such as birth certificates and social security cards, states may issue fraudulent licenses to criminals and terrorists. Under Real ID, states are required to check the validity of these documents by cross referencing with both federal and other state databases (Ramasastry, 2005). As many critics stated shortly after the initial passage of the Act, this requirement for breeder-document checking appeared to require the establishment of a federal system of records similar to the Chinese government's population registry database.<sup>25</sup> The U.S. government has been adamant in its position that it will not maintain any kind of central database as part of the Real ID program.

Chertoff said, "We at the Department of Homeland Security in the federal government will not build, will not own, and will not operate any central database containing personal information. The data will continue to be held at the state level as it has traditionally been since they began to issue driver's licenses. And by improving the quality of the documents, we're going to make it very, very much harder for people to forge them, counterfeit them, or alter them." (Moore, 2007, n.p.)

Given the range of possible information architectures for any system of records, the meaning of a "central database" has to be considered very carefully. To do this, let us first look in a bit more detail at specific requirements for ID issuance that the Real ID Act demands of states (PL 109-13). Section 37.13 identifies five different forms of document verification that the state must perform before issuing a REAL ID to an applicant:

1) any immigration documents issued by the DHS via Systematic Alien Verification for Entitlements (SAVE) system; 2) verify SSNs with the Social Security Administration (SSA) or through another method approved by DHS; 3) birth certificates, using Electronic Verification of Vital Events (EVVE) system or other electronic systems whenever the records are available; 4) documents issued by the Department of State with the Department of State or through methods approved by DHS; 5) States must verify REAL ID driver's licenses and identification cards with the State of issuance.

---

<sup>25</sup> Covered in more detail in chapter 6.

As of March, 2009, only two of the five verification systems that REAL ID requires were operational nationwide: 1) the Social Security verification System or (SSOLV) and the 2) Systematic Alien Verification for Entitlements (SAVE) system. A third system, Electronic Verification of Vital Events (EVVE) was in pilot stage. Of these three programs, two were being run by state agencies, the Social Security Administration (SSA) and DHS. The third, EVVE, is being administered by NAPHSIS, a non-profit association of state vital records and public health statistics offices. Since the first four of these SoRs are being developed independently of the Real ID system, the federal government can legitimately claim, at least with these SoRs, that they are not implementing a federal centralized database to support Real ID. For the fifth SoR, however, the Real ID verification system, such a claim is harder to make. In this case, the government is relying on a technical distinction, namely that any records in this new Real ID verification system will not be centrally stored.

For the Real ID system to protect the integrity of its identification credentials, it must never be possible for one person to obtain more than one card. Before a state issues a Real ID card, it must check the person's identity and confirm that no other states have issued a card to this unique identity. In other words, there needs to be a system of records that includes records for all REAL ID cards ever issued and the identities of the people to whom they were issued, and it must not involve central storage of this data under federal auspices.

In 2007, privacy activist Bill Scannell claimed to have obtained internal DHS documents which considered three scenarios for how such a system might be built (Singel, 2007d). If valid, they provide an important example of the kinds of architectures that DHS was considering and how they would all achieve their functionality without necessarily requiring the federal government to store personal information on all Real ID holders. The first scenario leaves the process of breeder document verification to the states themselves, maximizing state flexibility,

but is potentially “burdensome and chaotic in implementation.” The second scenario, known as the “federated” or “decentralized” system, would allow states to store and maintain control over their records with a standardized software interface implementing a “pointer” index telling states where they can find relevant information about applicants. A similar system for commercial driver’s licenses, the Commercial Driver’s License Information System (CDLIS), is already being operated by the Department of Transportation. In the third scenario, the states could use an intermediary, perhaps a private organization, to act as a clearinghouse, but again with no data being centrally stored. According to the document:

In none of these approaches would a large permanent multistate collection of individual records be created. The “federated” and clearinghouse alternatives are focused on the infrastructure among systems, and would not act as a substitute for the databases that hold the actual information (i.e., the databases would not “dump” into the clearinghouse) (“Real ID Snippet Unverified,” n.d.).

It now appears that DHS will be following the federated model based on the Commercial Driver’s License Information System (CDLIS). An AAMVA Real ID Verification Systems Working Group, working under the direction of the DHS has recommended “using a common platform for modernized CDLIS and a state-to-state verification system.” This will allow the DHS to move forward with the Real ID verification system while maintaining its promise that it will not store data on U.S. citizens in conjunction with the program. Data in this system may be accessible to a federal agent in Washington, but it will remain stored and maintained at the state level. This kind of architecture has become popular within other areas of the U.S. dossier system; as we will see later in the chapter, it is also the basic architecture used to facilitate the sharing of suspicious activity reports between state, local and federal agencies.

While there has been some progress in defining systems for the implementation of Real ID’s card issuing standards, at least in terms of outlining a basic architecture for the Real ID verification system, the overall five-part requirement remains far away from viability. These

specific requirements appear likely to die with the Real ID initiative, but the federal government has not given up its claimed right to dictate issuing standards in the future. Of more interest to the long term struggle over the NIDS are the use and physical characteristics of the card.

## 2) USE OF THE REAL ID

A critical factor in how any national supported ID system is experienced is the range of common life situations where one would be expected to present the card. Assuming the Real ID includes a unique numerical ID linked to a unique individual and is certified by the state, the more the Real ID is used, the more it will afford the production and centralized aggregation of PII. Requiring residents to carry an ID card at all times is clearly something associated with tyranny and oppression. As instances where demands for the card grow, the oppression associated with the card system will grow as well.

The Real ID Act, echoing the original clause in the Immigration Reform Act of 1996, states that “[b]eginning 3 years after the date of the enactment of this division, a Federal agency may not accept, for any official purpose, a driver’s license or identification card issued by a State” unless that state’s ID card meets the standards set forth in the Act. The official purposes of the Real ID card listed in the act are “accessing Federal facilities, boarding federally regulated commercial aircraft, entering nuclear power plants, and any other purposes that the Secretary shall determine.” Since this is a driver’s license, U.S. residents are also required to carry it whenever they are operating a motor vehicle. Although not stated in the original Real ID Act, numerous other uses of the card are suggested in the NPRM, including the presentation of the card for voting, applying for a job, receiving government benefits, and buying alcohol and cigarettes (72 FR 10820). A DHS official has even suggested that Real ID could be required for the purchase of some over the counter medicines as a way of combating the methamphetamine crisis (Broache, 2008).

The Immigration reform bill under discussion in the Senate (S 1348) in the summer of 2007 contained a Real ID mandate, requiring that employees get Real ID compliant IDs or passports from new hires for the purposes of verifying their identity and to store copies of them. As the Center for Democracy and Technology has pointed out, requiring a Real ID for employment puts to question the government claim that Real ID is a voluntary program (Cope, 2007).

The March, 2007 DHS NPRM on Real ID notes that “under the discretionary authority granted to the Secretary of Homeland Security under the Act,” that DHS “may expand this definition in the future,” and asks for public comment on “how DHS could expand this definition to other federal activities.”

The rule would give states, local governments, or private sector entities an option to choose to require the use of REAL IDs for activities beyond the official purposes defined in this regulation. To the extent that states, local governments, and private sector entities make this choice, the rule may facilitate processes which depend on licenses and cards for identification and may benefit from the enhanced security procedures and characteristics put in place as a result of this proposed rule. (72 FR 10845, 2007)

It is quite clear that the number of moments where both public and private entities demand the card for the provision of benefit or service, or simply demand provision to avoid arrest, will expand much as the use of the SSN expanded after its introduction in the mid 1930s. In addition to required state and federal uses, the decision not to specifically prohibit private entities from requiring presentation and scanning of the Real ID card will almost certainly lead to increases in situations where the card is demanded for service.

### 3) COMPOSITION AND CONTENT OF THE CARD

Generally under IRPTA (2004) and more specifically under Real ID Act (2005), the federal government has assumed authority to dictate certain physical aspects of the state driver's license such as the particular use of a biometric or other identification scheme. The federal

government also assumes the right to dictate certain types of information that must be included. To meet the requirements of section 202(b) of the Act, a State is required to include, at a minimum, the following information and features on each driver's license and identification card: (1) Full legal name; (2) Date of birth; (3) Gender; (4) Driver's license or identification card number; (5) A digital color photograph; (6) Address of principal residence; (7) Signature; (8) Physical security features designed to prevent tampering, counterfeiting, or duplication of the document for any fraudulent purpose; (9) A common machine readable technology (MRT), with defined minimum data elements. States must also include the issue date and expiration date on each card (72 FR 10820, 2007).

The MRT referred to in the Real ID rule and in the Act itself has been the most controversial aspect of the Real ID plan among privacy advocates. Intended to allow basic information on the card to be read and entered into a processing system automatically, the specific form of MRT was not specified in the original Real ID Act, leading many to speculate on a range of possibilities. Most controversial among these possibilities was the use of an RFID tag:

To anyone who's clued in about RFID, the spychipped driver's licenses are a complete privacy nightmare. They can be silently read from 20-feet away, through a person's wallet, pocket, backpack, or purse — even when the target is in a moving car. They are unencrypted and contain a unique ID number that can be used to identify and track people miles from the border — indeed, anywhere the government chooses to put a reader.

But it's not just the government that could use the cards to track and surveil people. Anyone with a rudimentary RFID reader can remotely access the the unique ID number on the card. Retailers could use them to ID customers as they walk in the door. Marketers could use them to track people around the store. Stalkers could use them to track their victims. Terrorists could scan for them in crowds and pinpoint Americans traveling in other countries. Hackers could duplicate the signal emitted by chipped licenses to impersonate people. The list of potential abuses for the ill-conceived ID card are staggering. (Albrecht, 2008, n.p.)

In the midst of widespread public condemnation of this possibility, the DHS, in the March, 2007 NPRM, announced that it had decided not to require the use of RFID in its Real ID standard:

The integrated contactless chip was not deemed an appropriate technology for this particular document, as there is not an identifiable need for driver's licenses and identification cards to be routinely read at a distance. (72 FR 10820, 2007, p. 10837)

One of the major claims to victory here was that public resistance stopped the DHS from attempting to require RFID chips in Real ID, forcing a lower technology standard that did not afford simple electronic eavesdropping: the 2D barcode. It would be hard to overstate how partial this victory was. First, the 2D barcode, while requiring a line of sight to be read, was unencrypted and could be read by any private individual or organization with basic barcode reading technology. Further, not only did the DHS retain the right to update rules at a later date and require RFID in Real ID, but they were also already in the process of issuing tens of thousands of identity documents with embedded RFID, from passports to pass cards to Enhanced Driver's Licenses (EDLs). As we will see, the government decided to make these design choices despite overwhelming public sentiment against the technology.

The decision not to include RFID in the Real ID program was made shortly after the unsuccessful trial of RFID tags in DHS I-94 immigration forms. In 2006, the DHS ran a trial of RFID tags in forms used in the U.S. VISIT program at five points of entry at the northern and southern borders. In the trial, RFID readers were placed above the inspection lanes, intended to read the tag information as people passed under them. The test showed "numerous performance and reliability problems:"

For example, according to U.S.-VISIT, at the Blaine-Pacific Highway test site, of 166 vehicles tested during a 1-week period, RFID readers correctly identified 14 percent — a sizable departure from the target read rate of 70 percent. (U.S. GAO, 2007, January 31, p. 18)

When the trial was finished, the ability of the readers to read the tags was too unreliable to warrant continuing with the I-94 RFID project. The decision to abandon RFID within the U.S. VISIT program was confirmed by Chertoff in February 9, 2007 congressional testimony.

“I mean, this is the real world,” Chertoff said. “I think, yes, we’re abandoning it. That’s not going to be a solution. So in the real world, when something fails, we drop it and we move to the next thing,” he added. (Lipowicz, 2007d, n.p.)

A month later in the Real ID NPRM, the DHS officially abandoned any plans to require RFID (called contactless chips in the document) within Real ID cards. In the context of the recent U.S. Visit test failure and widespread public condemnation of RFID in personal ID cards, it appeared that privacy advocates had won a major victory:

“CAGW activists successfully thwarted RFID-based licenses, saving taxpayers \$4.4 to \$8.4 billion and heading off a grave risk to privacy. However, REAL ID remains problematic. It is an unfunded mandate on the states, and despite DHS statements to the contrary, moves the country closer to a national ID card,” Schatz concluded. (“CAGW: Real ID Regulations,” 2007)

Although RFID is not part of the final standard for Real ID, it is included in at least three different types of federally-administered or federally-approved identity credentials: the U.S. passport book, the U.S. pass card, and the Enhanced Driver’s License. The government’s decision to implement RFID, in each case, was made despite clear and vocal public rejection of the policy.

In February, 2005, the U.S. State Department requested public comment on its proposal to introduce electronic passports with embedded RFID chips. According to the State Department, more than 98 per cent of the 2335 public comments received were negative, many of them citing privacy and security concerns (Gross, 2005).

In October 2006, the DHS Data Privacy and Integrity Advisory Committee, an independent committee established by the DHS to provide “advice at the request of the Secretary of Homeland Security and the DHS Chief Privacy Officer on programmatic, policy, operational,



administrative, and technological issues within the DHS that relate to personally identifiable information, as well as data integrity and other privacy-related matters,” (“Privacy Office,” 2009, n.p.) produced a draft report advising against the use of remotely read RFID chips in identity documents:

There appear to be specific, narrowly defined situations in which RFID is appropriate for human identification. Miners or firefighters might be appropriately identified using RFID because speed of identification is at a premium in dangerous situations and the need to verify the connection between a card and bearer is low.

But for other applications related to human beings, RFID appears to offer little benefit when compared to the consequences it brings for privacy and data integrity. Instead, it increases risks to personal privacy and security, with no commensurate benefit for performance or national security. Most difficult and troubling is the situation in which RFID is ostensibly used for tracking objects (medicine containers, for example), but can be in fact used for monitoring human behavior. These types of uses are still being explored and remain difficult to predict.

For these reasons, we recommend that RFID be disfavored for identifying and tracking human beings. (U.S. DHS, 2006, October, p. 1)

According to committee member and Cato Institute fellow Jim Harper, the DHS quietly shelved the project report without letting it out of draft stage.

“The powers that be took a good run at deep-sixing this report,” Harper said. “There’s such a strongly held consensus among industry and DHS that RFID is the way to go that getting people off of that and getting them to examine the technology is very hard to do.” (Singel, 2006, n.p.)

In the same month, on October 17, the State Department solicited public comments in the *Federal Register* (71 FR 60928, 2006) on its proposed choice of proximity RFID technology for its new passport card, a cheaper version of the passport that could be used for travel within North America. When the final rules for the passport card were issued more than a year later, DHS noted that 4000 comments had been received, with the “vast majority” opposed to the use of proximity RFID technology within the cards. Of the 4000 submissions, approximately 20 comments specifically voiced support for the passport card. Despite the overwhelming public

sentiment against the use of proximity RFID, the DHS announced that passport cards would utilize RFID:

While State and DHS appreciate the comments received, the vast majority reflected an improper understanding of the business model that WHTI [Western Hemisphere Travel Initiative] is designed to meet and how the technology selected would actually be implemented. DHS remains committed to vicinity-read radio frequency identification (RFID) as the most appropriate technological solution to facilitate document processing at land and sea ports-of-entry. Vicinity-read RFID technology should allow CBP officers to quickly obtain information about the border crosser and perform terrorist watch list checks while they are still awaiting a personal inspection and to read multiple cards simultaneously. Therefore, to ensure compatibility and interoperability with the DHS border management system, and to secure significant travel facilitation advantages, the Department of State will produce the passport card utilizing vicinity RFID technology. (72 FR 74169, 2007).

While the data privacy committee report sat in draft stage and despite overwhelmingly negative public comment on the proposal, the U.S. continued its program for introducing RFID into citizen identity documents. By 2007, citizens driving across the Canadian border could no longer use their normal driver's license but needed to have their passport or one of the newly developed Pass Cards, an identity card with an embedded RFID chip that can be read from over 20 feet away.

The goal of the passport card, an alternative to the traditional passport, is to reduce the wait at land and sea border checkpoints by using an electronic device that can simultaneously read multiple cards' radio frequency identification (RFID) signals from a distance, checking travelers against terrorist and criminal watchlists while they wait. "As people are approaching a port of inspection, they can show the card to the reader, and by the time they get to the inspector, all the information will have been verified and they can be waved on through," said Ann Barrett, deputy assistant secretary of state for passport services, commenting on the final rule on passport cards published yesterday in the *Federal Register*. (Nakashima, 2008, n.p.)

More significant is the new program of Enhanced Driver's Licenses (EDLs) that also use the newer, proximity RFID technology. As we will see, this could represent an end around strategy for the U.S. government to phase in national ID cards with embedded RFID.

## ENHANCED DRIVER'S LICENSE

The Western Hemisphere Travel Initiative (WHTI), passed by Congress and signed into law as part of the Intelligence Reform and Terrorism Prevention Act of 2004, will, as of June 1, 2009 require travelers from Canada, Mexico, the Caribbean and Bermuda, including U.S. citizens, to present a passport or Enhanced Driver's License (EDL) to enter the United States. The EDL also functions as a regular driver's license, but meets specific federal requirements including the use of RFID technology. Travelers in the past have been exempt from such requirements and could simply show driver's licenses produced according to local standards, whether the locality was a province in Canada or a U.S. state. As the DHS indicates, it is encouraging states to "enhance" their driver's licenses to meet WHTI requirements:

DHS is pursuing development of alternative documents to meet Western Hemisphere Travel Initiative (WHTI) implementation requirements at land and sea ports of entry. DHS is encouraging states to submit proposals to enhance their driver's licenses and identification documents to satisfy WHTI requirements. ("Fact Sheet: Enhanced Driver's Licenses," 2007, n.p.)

Current U.S. AG Janet Napolitano, who signed one of many state bills outlawing Real ID, is an advocate of the EDL:

"Enhanced driver's licenses give confidence that the person holding the card is the person who is supposed to be holding the card, and it's less elaborate than Real ID," Miss Napolitano said. (Hudson, 2009, n.p.)

As of early 2009, the EDL was in use or being planned for 7 states, comprising roughly 30 per cent of the U.S. population. In Washington State, where the program was first piloted, more than 2,000 signed up for EDLs in the first two days of the program ("2,000 Sign up," 2008).

Whether or not the Real ID Act gets revised and redeployed or fades into obscurity, the U.S. government continues to advance and strengthen its nationwide identity system program. The failure of Real ID does not mean that the federal government has given up on its goal of building a nationwide information system to verify the authenticity of breeder documents like

birth certificates and passports; it does not mean it has given up its newly claimed authority to dictate situations which should require presentation of a federally authorized card, nor does it mean it will decide to regulate or restrict private uses of the ID card. Most importantly, whatever Real ID victory card there was, it has little to do with the struggle to keep RFID tags out of federally approved identity documents. The Intelligence Reform and Terrorism Protection Act of 2004, which asserts this federal authority, remains in effect regardless of the fate of the Real ID Act.

Ultimately, though much of the Real ID struggle appears to be documented with this searchable SIP, “Real ID,” it is very likely that the name itself will become less relevant over time. The primary SIP for exploring the struggle over a national ID system may soon be “Enhanced Driver’s License” rather than Real ID.

As we consider the SoR section to follow, it is important to remember that, although they can greatly facilitate the states production and collection of PII, a definitive national ID system is not a necessary component of problematic state dossier configurations.

## SYSTEMS OF RECORDS

This section is divided into three sections, the first covering a major SoR, the *Investigative Data Warehouse*, and the second two sections covering important types of records that flow across record systems: *suspicious activity reports* and *watch lists*.

### INVESTIGATIVE DATA WAREHOUSE

What is the Investigative Data Warehouse (IDW)? Public officials both inside and outside the FBI itself have often confused or conflated the IDW with a number of other FBI systems, initiatives and projects, including “Project Trilogy,” the “Virtual Case File System,”

Sentinel, and “Project Z.” Just prior to its official launch, FBI director Mueller introduced the project to Congress as the Integrated Data Warehouse but it has since been referred to explicitly as the Investigative Data Warehouse. Inconsistencies in terminology, even by officials who direct the programs, can create ripples of confusion among researchers and activists.

The IDW began first as a pilot project known as the Secure Counterterrorist Operational Prototype Environment (SCOPE) program before being officially launched under the IDW name in January of 2004. The data warehouse is related to, but not formally part of, the Trilogy project. The Trilogy project, officially launched in November of 2000, was the FBI’s congressionally funded project to upgrade the agency’s outdated IT systems (U.S. FBI, 2004). Trilogy, which received an initial allocation of \$379 million from Congress, was divided into three components. The first two components, upgrades to the FBI’s computer networking system and all computer hardware, were completed in April 2004. The third component of the project, the upgrading of the agency’s antiquated case software, the Automated Case System (ACS), with a Virtual Case File system (VCF), was never completed due to management and technology problems (Anderson, 2005).

The Investigative Data Warehouse, according to the FBI’s 2004 report to the 9/11 Commission, “contains all data that can legally be stored together” (U.S. FBI, 2004, p. 54). According to congressional testimony delivered by FBI director Robert Mueller on Feb 3, 2005, the IDW at that time included “47 sources of counterterrorism data, including information from FBI files, other government agency data, and open source news feeds that were previously available only through separate, stove-piped systems” (Mueller, 2005, n.p.). In December of 2006, Senator Patrick Leahy stated that the IDW contained “over half a billion FBI and other agency documents” and could be accessed by more than 12,000 users in federal, state and local law enforcement (Leahy, 2006).

The IDW physically stores the data that it aggregates, rather than simply acting as a gateway to other record systems. A complete accounting of data sources feeding into the IDW has never been made available to the public. Although privacy advocates including the EFF and EPIC have claimed that the FBI is in violation of the Privacy Act for not filing a SORN in the *Federal Register*, the FBI argues that since no new data is created by the IDW, it does not meet the legal definition of a “system of records” and thus the Privacy Act does not apply. According to FBI spokesman Paul Bresson, the IDW “simply unifies previously and lawfully acquired data from other established databases into one place” (Caterinicchia, 2006, n.p.). Based on congressional testimony and other public statements from FBI personnel, we know that data for the IDW comes from the following agencies: the Treasury Department, the State Department, the Department of Homeland Security, the Department of Defense, the CIA, the NSA and the National Counter Terrorism Center. Specific records it is aggregating include the No Fly list maintained at the Terrorist Screening Database (TSDB), suspicious activity reports submitted by bankers to the Treasury Department’s Financial Crimes Enforcement Network (FINCEN), the list of missing or stolen passports maintained by the State Department, and all databases maintained by agencies within the Department of Justice. Data can be retrieved from the IDW using a wide range of personal identifiers at speeds several orders of magnitude faster than was once possible with legacy systems:

An agent who has to run a search of a thousand names of potential suspects, for example, can now do so in 30 minutes, even with all variations of names, dates of birth and Social Security numbers. That same search, through the once-separate 18 databases, used to take 32,000 hours. The system is also set up so that variations in names and dates, which differ from agency to agency, and country to country, can be searched easily. This means that leaving off the “19” in a year of birth, for example, won’t keep the FBI from missing a huge lead. (Todd, 2006, n.p.)

The IDW appears to be performing many of the functions of the legacy ACS case management system that the abortive VCF project was supposed to replace. Much, but not all of

the data entered into the ACS system, is also stored in the IDW. Although it seems clear that the IDW, at least for the time being, is being used to distribute case files, FBI spokespeople are careful to point out that, as of yet, no replacement has come online for ACS. In addition, data gathered by FBI agents using National Security Letters is also stored within the IDW.

How broad is the coverage of the IDW? What percentage of American citizens is included in the database? Given the paucity of publicly available information, this is a difficult, if not impossible question to answer. A reporter for the *San Francisco Chronicle*, doing research for an article about the FBI, found that the IDW had detailed records on his own life:

Up popped my name in an investigation of Scott Ritter, the former top Iraq arms inspector turned administration critic. I'd interviewed him on the telephone several times in the late 1990s.

Scrolling down, I also saw a note on my 1972 membership in a group of graduate students and faculty who wrote scholarly articles against the war in Vietnam, evidently related to an investigation of Jane Fonda. There were also excerpts of articles I'd written over the years that mentioned bombings and the FBI.

And there were what looked like my bank transactions, past addresses and telephone numbers.

This was a lot more information about me than the FBI said they had when I requested my files in the late 1990s. And from my cursory peek, I could tell my files went deep. (Stein, 2006, March 5)

Further, given the expanded use of National Security Letters by the FBI to retrieve information about clients and customers of private companies, and the current policy allowing agents to retain information collected on innocent people for possible future intelligence value, it appears likely that coverage goes beyond convicted criminals and suspected terrorists.

The FBI has indicated that it does not see the IDW as the ultimate, one stop database for the bureau. The system term that has been reserved for this ultimate data storage system is the "Master Data Warehouse" (MDW). At some future date, according to the FBI's 2004 report to

the 9/11 commission, the Master Data Warehouse will become “the system of record for, all FBI electronic files” (U.S. FBI, 2004, p. 54).

#### ROLE OF THE PRIVATE SECTOR

Given the considerable scope of the IDW, it is important to consider the major loophole around the Privacy Act. Since there is no omnibus privacy law other than the Privacy Act, and since legal restrictions on private information sharing are sector specific, a wide range of personal data may be legally provided from the private to the public sector, either voluntarily or for a fee. While some Privacy Act restrictions do apply to government contractors, this appears only to hold when the associated database is produced directly under state direction, not when a private entity makes available already existing data (“Privacy’s Gap,” 2003).

A wealth of documentary evidence confirms that the FBI has made long term and expanding use of data from private data-mining and telecom firms, including, by its own admission, Choicepoint, Verizon, ATT and MCI (O’Brian, 2007). Following revelations that it was sharing data with the NSA’s terrorist surveillance program, ATT released an update to its privacy policy that it appeared designed to provide the shield the company from any further legal fault finding (Lazarus, 2006).

At the Open Data 2007 conference in Manhattan, the CTO of a web market research firm confirmed that ISPs large and small were selling their click stream data to third parties. Although this data is supposedly anonymized to protect the privacy of individual consumers, reidentifying virtually all of the data subjects would be trivial given the comprehensive nature of the data. The technology web site *Ars Technica* notes that it is “theoretically possible” to tie the information back to a specific ISP account.



The data is not sold with accompanying user names or information but merely as a numerical user value. However, it is still theoretically possible to tie this information to a specific ISP account. Cancel told Ars that his company licenses the data from ISPs for millions of dollars. He did not give a specific figure about what this broke down to in terms of dollars per ISP user, although someone in the audience estimated that it was in the range of 40¢ per user per month—this estimate was erroneously attributed to Cancel himself in some reports on the event. Cancel said that this clickstream data is “much more comprehensive” than data that is normally gleaned through analyzing search queries. (Reimer, 2007, n.p.)

It is interesting to note that while government agencies are required (with certain exceptions) to notify the public via the *Federal Register* for the creation of a new SoR, private companies such as ISPs are under no such obligation. The desire to aggregate full spectrum information on a person, to produce their dossier, may spring from different social actors, interests and goals. A new practice in financial risk indexing, “identity scoring,” makes an argument for aggregating and processing an individual’s comprehensive data shadow to predict their range of possible behaviors and more easily identify those attempting to fraudulently use an identity. Although one might assume that a credit score index cares only about an individual’s financial information, innovations in financial risk management are calling for access to a much wider range of data:

Identity scoring works on the same principle as other behavioral scoring systems such as credit scoring or auto insurance scoring — it aggregates data on individuals from various sources and uses predictive analysis to generate a model of behavior.

Unlike typical credit monitoring, identity scoring utilizes all of the available data on an individual to make its judgment; everything from law enforcement records to property deeds to Internet chat logs can be used to generate an identity score. The end results are much more specific and capable of accurately judging a person’s information as being authentic.

Identity scoring systems can be used to monitor all types of personal information, including debit card and Social Security number use — and misuse. They enable monitoring of individual behavior across multiple enterprises, over periods of time, to create the most accurate profile possible of a person’s activities (Kraft, 2007, n.p.).

By allowing a private firm to maintain their “identity score” they can be freed from the danger of identity theft, at least until the criminals crack the scores and modify their own

behavior accordingly, so as not to deviate from the expected behavior of their victim. The problem of course, is that once this dossier has been produced, it may be acquired by other actors whose interests in the data may deviate from and even directly oppose that of the data subject.

An organization designed to promote social ties between CEOs of critical infrastructure industries and the FBI, the InfraGard<sup>26</sup>, provides another set of channels in which private sector PII, in the form of suspicious activity reports, may be transferred to the federal government without significant oversight. Much of this data could wind up in the IDW, whether or not a particular data subject is suspected of having committed a crime.

### SUSPICIOUS ACTIVITY REPORTS

What is a Suspicious Activity Report (SAR)? If one were to rely on Wikipedia as of April 23, 2009, one would come to the conclusion that SARs are a practice limited to the financial sector:

A Suspicious Activity Report (or SAR) is a report regarding suspicious or potentially suspicious activity, filed with the Financial Crimes Enforcement Network (FinCEN), an agency of the United States Department of the Treasury.

The purpose of the Suspicious Activity Report is to report known or suspected violations of law or suspicious activity observed by financial institutions subject to the regulations of the Bank Secrecy Act (BSA). In many instances, SARs have been instrumental in enabling law enforcement to initiate or supplement major money laundering or terrorist financing investigations and other criminal cases. Information provided in SAR forms also presents FinCEN with a method of identifying emerging trends and patterns associated with financial crimes. The information about those trends and patterns is vital to law enforcement agencies and provides valuable feedback to financial institutions. (Wikipedia, “Suspicious Activity Report”)<sup>27</sup>

The Wikipedia entry includes one small warning text that reads “[t]he examples and perspective in this article may not represent a worldwide view of the subject,” but otherwise there

---

<sup>26</sup> Covered later in the chapter.

<sup>27</sup> Retrieved April 23, 2009 from [http://en.wikipedia.org/wiki/Suspicious\\_activity\\_report](http://en.wikipedia.org/wiki/Suspicious_activity_report)

is no mention that the definition of SAR is several years out of date. More comprehensive, up-to-date information about the national suspicious activity reporting requires a more thorough search.

According to the program manager of the office of the Information Sharing Environment, the SAR is an electronic file produced by a rapidly growing number of state agents as part of a large scale government initiative to make sure that “most Federal, State, local, and tribal law enforcement organizations will participate in a standardized, integrated approach to gathering, documenting, processing, analyzing, and sharing information about suspicious activity that is potentially terrorism-related.”<sup>28</sup> As this section will show, Suspicious Activity Reports (also known as Surveillance Detection Reports (SDRs)) are being produced at a rapidly accelerating rate, not only within the financial sector, but in the police, military and private business sectors as well.

The SAR represents a dramatic expansion of the role of domestic intelligence in the U.S., more wide spread than such activity was at the height of FBI, CIA and military abuses uncovered during the 1973 Church Committee hearings. The emerging SAR is none other than a wholesale return of the kind of dossier production and record sharing that was both condemned in public and constrained in policy by both law and official guidelines. This represents a radical shift in roles for more than eight hundred thousand local police officers, who are now being asked to serve as an extension of FBI intelligence apparatus, along with a growing contingent of private sector informants from InfraGard members to Terrorist Liaison Officers<sup>29</sup>, all of them the eyes and ears of a new domestic intelligence apparatus under the guidance of the Department of Homeland Security.

---

<sup>28</sup> Information Sharing Environment website on SAR initiative, retrieved 8/1/09 from <http://www.ise.gov/pages/sar-initiative.html>

<sup>29</sup> Both InfraGard and Terrorist Liaison Officers are covered later in the chapter.

Though specific numbers are hard to come by, it is clear that the number of individuals whose “reports” are feeding into the domestic intelligence system is growing rapidly and is already unprecedented in American history. This particular class of PII, PII of state suspicion, tends to persist within information systems longer than files of specific criminal investigation (Treverton, 2008) and circulates through a network of record systems, where some of them become triggers for the production of watch lists and other “persons of interest” lists. The Suspicious Activity Reporting (SAR) system, as we will see, leads to the production of PII that is often woven into the state’s counterterrorism narrative. Innocent people on the street engaging in First Amendment activities or simply minding their own business may be “interpellated” (Poster, 1996) into a government counter terrorism database within a narrative of suspicion and threat.

Before looking in detail at the current sites (institutional, technological, locational) and logics of the SAR, I present some important recent historical context. First, I offer some background on the financial SAR referenced in the Wikipedia entry. The Financial SAR was the first major SAR form and is still the most thoroughly accounted for in government documents. Next, I discuss two recent events that help us to better understand what is happening today: 1) The TIPS program and 2) the fall 2006 TALON scandal, in which evidence surfaced demonstrating the U.S. Military had been spying on and creating files on Americans engaged in First Amendment activities.

#### FINANCIAL SUSPICIOUS ACTIVITY REPORT

The most well-established form of SAR within the U.S. is the financial SAR, first required as part of the (amended) Banking Secrecy Act in 1996. The original act required any transaction over 10,000 to be reported to the federal government. In 1997, the notion of “suspicious activity report” was introduced for transactions over \$5000 in which there was suspicion of crime or a link to terrorism. Originally banks, and now a wide range of institutions

involved in money-related services (including gambling casinos and precious metal dealers) must file SARs whenever they have even the slightest suspicion that banking activity carried out by a customer may be related to criminal or terrorist activity. *The Comptroller's Handbook*, published in 2000, describes a number of scenarios in which they recommend the banker file a SAR. They include:

- A customer's corporate account(s) has deposits or withdrawals primarily in cash rather than checks.
- The owner of both a retail business and a check cashing service does not ask for cash when depositing checks, possibly indicating the availability of another source of cash.
- The customer engages in unusual activity in cash purchases of traveler's checks, money orders, or cashier's checks.
- A spike in the customer's activity with little or no explanation. (U.S. DOT, 2000, pp. 12-15)

In 2004, Riggs Bank was fined \$25 million for failing to crack down on money laundering activities. In 2005, ABN AMRO bank was forced to pay \$80 million. Wanting to avoid financial liability for non filing and protect themselves from liability for unnecessarily filing reports, banks increasingly err on the side of "caution," filing whenever customer activity has the slightest tinge of suspicious behavior (Bruce, 2006). The number of financial SARs produced within the United States has risen steadily, from 62,000 in 1996 to more than 1 million in 2005. Once submitted, SARS are sent to and stored within the Financial Crimes Enforcement Network (FINCEN) maintained by the Treasury Department and shared with other agency systems of records such as the FBI's Investigative Data Warehouse (IDW) (U.S. GAO, 2006, June 12).

#### TERRORISM INFORMATION & PREVENTION SYSTEM (TIPS)

The Terrorism Information & Prevention System (TIPS), introduced by Attorney General Ashcroft as part of President Bush's Freedom Corps initiative, and originally set to launch in

August 2002, was presented as the government's front line protection against terrorism. The TIPS system would deputize millions of American workers to be on the lookout for suspicious activity. Specifically, the TIPS program looked to enlist "American workers who, in the daily course of their work, are in a unique position to see potentially unusual or suspicious activity in public places" (Mathews, 2002, July 29). Among the professions targeted were meter readers, truck drivers, mail carriers and train conductors. A pilot program was set to begin with one million informants in ten cities, more than 4% of their aggregate population. TIPS volunteers would be given a special toll-free telephone number and web site where they could submit reports of any suspicious behavior.

Reaction to the proposed program was overwhelmingly negative. Newspapers editorials pointed out that the percentage of citizen spies in the TIPS program would exceed that of cold war East Germany's notorious Stasi program. *New York Times'* columnist William Safire galvanized opposition with his November 14 column, "You are a Suspect." CNET columnist Lisa Bowman asked, "Is Your Cable Guy a Spy?" (Bowman, July 17, 2002).

Many expressed concern about whether the reports of suspicious activity would find their way into a massive government database. Testifying before congress in late July, Ashcroft said he advised against creating a database that would be maintained by Operation TIPS, and "I have been given assurances that TIPS will not maintain a database." But the FBI and other agencies might preserve TIPS reports in databases, he said. (Mathews, 2002, July 29)

The DOJ quickly responded to the criticisms, scaling back the program to specifically eliminate those workers, who through their daily jobs, had access to people's homes. An email sent to TIPS volunteers in early August told them they would no longer be needed and that the

program would now be limited to “only those who work in the trucking, maritime, shipping, and mass transit industries” (Lindorff, 2002, August 30, n.p.).

Still, concern over the impact of the program on civil liberties remained high. House Majority Leader Dick Armey (R-TX) and Senate Patrick Leahy (D-VT) came out strongly against the scheme. Armey placed a measure within that fall’s Homeland Security bill explicitly defunding the program. Although Leahy supported the defunding measure, Senator Joe Lieberman, chairman of the Homeland Security committee, was able to keep the measure out of the Senate version.

The overwhelmingly negative reaction to the program helped sap its momentum, and Operation TIPS was quietly shelved. As we will see, however, the basic components of this system continue to be developed. The notion of leveraging the public at large to act as source for data on suspicious, potentially targeted persons has been “in development” both practically and conceptually, ever since.

#### JOINT PROTECTION ENTERPRISE NETWORK (JPEN)

The Joint Protection Enterprise Network (JPEN) was a computer network designed for the sharing of unclassified “force protection” information between military installations. The network, operated by the United States Northern Command, the division of the U.S. military entrusted with protecting the U.S. homeland since October 1, 2002, stored and distributed reports regarding known or suspected suspicious activity and incidents at, or somehow threatening, DoD installations. According to a 2004 report in the Armed Forces Communications and Electronics Association’s *SIGNAL* magazine, “JPEN has changed hands and names several times since its inception” (Lilie, 2004, n.p.).

According to the JPEN SORN published in the *Federal Register* on September 23, 2003, the database could store information on “[a]ny individual, civilian or military, involved in, witnessing or suspected of being involved in or reporting possible criminal activity affecting the interests, property, and/or personnel on a DoD installation.” Information stored within the system included “subject’s name, aliases, Social Security Number, address(es), telephone number, date of birth, driver’s license number, passport number, license plate number, vehicle description, description of occupants, source of investigation, risk analysis, threat assessment, victim names, names of informants, names of law enforcement officers and investigators, and subject’s group affiliations, if any” (68 FR 55593).

A key component of the JPEN system was the Threat and Local Observation Notice (TALON) report, a web-based entry form, originally developed as part of the Air Force’s Eagle Eyes threat notice system. In May, 2003, recognizing the need for a DOD wide standard, the Deputy Secretary of Defense established the TALON report as the “formal mechanism for assembling and sharing non-validated domestic threat information among intelligence, counter intelligence, law enforcement, security and force protection entities” (U.S. DOD, 2003, May 2, n.p.). TALON reports were generated when one of seven criteria, each with varying degrees of specificity, were met. The most specific threats included “tests of security” “bomb threats,” “surveillance,” “repetitive activities,” and “elicitation,” any attempt to obtain information from security or military personnel by unauthorized individuals. Two more general criteria were “non-specific threats,” and “suspicious activities or incidents” (Porter & Crumley, 2006, p. 26).

TALON agents were not trained to target individuals first. Instead, they were trained to be on the lookout for any suspicious behavior potentially indicative of a future threat. The general idea was that when the agent witnessed a suspicious event, they were supposed to generate a report. In practice, agents responsible for generating TALON reports made broad use of these



final two categories, generating and storing reports on constitutionally protected First Amendment activities including non-violent association and public assembly.

TALON included multiple source vectors for report data, including the public at large via special tip line. Trained agents then entered TALON reports with relevant data. These reports became available to other agents as “unverified data” and also flowed “up stream” to systems which vetted these unverified reports, deciding whether or not they warranted further investigation (Isikoff, 2006).

Chairman of the Joint Chiefs of Staff General Richard B. Myers first began to talk publicly about the JPEN system in the spring of 2004. Speaking at the AFCEA Technet International Conference on May 11, 2004, Myers conveyed his enthusiasm to the assembled crowd, suggesting that JPEN had a broader future than just protecting military installations:

How many of the folks in this room know anything about JPEN? If you don't know about JPEN, then you've got to go take a look at it. The Joint Protection Enterprise Network, it can be focused on anything, but right now, we're focused on security at military installations. (Myers, 2004, May 11, n.p.)

The following day, in testimony before Congress, Myers continued to hint at larger plans for the unclassified threat information network, stating “[a]though currently operating only on military installations, JPEN has the potential to be expanded to share terrorist information with Federal, State and local agencies as well” (Myers, 2004, May 12, n.p.). Soon, the DOD did begin to share “terrorist information” with the FBI, but not until the JPEN network and its associated TALON reports became embroiled in considerable controversy.

JPEN was operated under the direct management of a newly minted DOD agency, the Counter Intelligence Field Activity (CIFA), established per directive of the Secretary of Defense, Donald Rumsfeld on February 19, 2002. CIFA's declared mission was to “transform” the way counterintelligence is done “fully utilizing 21<sup>st</sup> century tools and resources” (Pincus, 2005). The

development of threat assessments by CIFA agents involved the exploitation of commercial data and the use of open-source intelligence (OSINT) such as publicly available web sites.

Between March 2004 and December 2005, CIFA had awarded more than 33 million dollars in contracts to “corporate giants Lockheed Martin, Unisys Corporation, Computer Sciences Corporation and Northrop Grumman to develop databases that comb through classified and unclassified government data, commercial information and Internet chatter to help sniff out terrorists, saboteurs and spies.” Although CIFA’s size and budget were classified, congressional sources told *Washington Post* reporter Walter Pincus that it had spent more than \$1 billion through October, 2006. A counterintelligence official estimated that CIFA, at the time, had more than 400 full-time employees and 800 to 900 contractors (Pincus, 2007, April 25, n.p.).

In November 2005, the White House proposed expanding the powers of CIFA, creating an intelligence exception to the Privacy Act that would allow the FBI and other agencies to share data about U.S. persons with the DOD, CIA and other intelligence agencies, “as long as the data is deemed to be related to foreign intelligence.” NBC reporters Lisa Myers, Douglas Pasternak, and Rich Gardella said CIFA “is becoming the superpower of data mining within the U.S. national security community” (Myers, Pasternak & Gardella, 2005, n.p.).

While the White House was formally pursuing an expansion of powers, CIFA personnel were already actively compiling reports on U.S. persons with and without direct connections to foreign intelligence. Making liberal use of the general TALON categories of suspicious activity, agents compiled written reports on U.S. citizens involved in anti-war protests and peace groups.

In the fall of 2005, investigative reporters and civil rights organizations began to take a strong interest in the activities of CIFA and the nature of their TALON reports. Their findings, first broadcast publicly on NBC Nightly news, quickly put the White House and the DOD on the

defensive. The December NBC investigative report published information showing that the DODs CIFA had been collecting TALON reports on anti-war groups and other non-violent groups. According to the initial NBC report, a 400-page document obtained from the DOD contained information on planned protests and other activities of “nearly four dozen anti-war meetings or protests.” Even when notations within the document indicated that a particular event was not deemed a credible threat, such as a protest against the draft in Fort Lauderdale in which the agent writes “U.S. group exercising constitutional rights,” they remained in the database anyway, including the names of particular identified people. As many government critics were quick to point out, this appeared to violate a long-standing (1982) DOD directive limiting collection of data on American citizens (Myers, Pasternak & Gardella, 2005, n.p.).

The Defense Department reacted quickly to the press reports, stating that it viewed “with the greatest concern any potential violation of strict DoD policy governing authorized counter-intelligence efforts and support to law enforcement,” and noted that its own regulations required that information not validated as threatening be “removed from the TALON system in less than ninety days.” A Pentagon statement released to the *FAS Secrecy News* announced that a review of the TALON reporting system had been underway since October and that the Under Secretary of Defense for Intelligence had directed several actions after the initial assessment of the database:

- \* First a thorough review of the TALON reporting system to ensure it complies fully with DoD and U.S. laws;
- \* Second, a review whether those policies and procedures are being properly applied with respect to any reporting and retention of information about any U.S. persons;
- \* Third, a review of the TALON data base to identify any other information that is improperly in the data base;
- \* Finally, all Department counterintelligence and intelligence personnel will receive immediate refresher training concerning the laws, policies and procedures that govern collection, reporting and storing of information related to the warning of potential threats to DoD personnel, facilities or national security interests. (“Pentagon Statement on Domestic Intelligence Surveillance,” 2005)

Even before the results of the investigation were released, DoD spokesman Bryan Whitman told Pentagon reporters “[I]t appears as if there may have been things that were left in the database that shouldn’t have been left there” (Gilmore, 2005, n.p.). In March, the DOD issued a memorandum, “Threats to the Department of Defense,” directing DOD personnel to generate Talon reports “for possible international terrorist activity” (U.S. DOD, 2006, March 30). A bit more than a year later, the Under Secretary of Defense for Intelligence requested that the TALON program be terminated “because the results of the last year do not merit continuing the program as currently constituted, particularly in light of its image in the Congress and the media” (U.S. DOD, 2007, June 27, p.14). In June, 2006 the JPEN system itself was recommended for closure by the commander of Northcom for budgetary reasons (U.S. DOD, 2007, June 27).

In June, the DOD Inspector General issued its report on CIFA and the TALON reporting system (U.S. DOD, 2007, June 27). According to the inspector’s findings, CIFA “legally gathered and maintained U.S. person information on individuals or organizations involved in domestic protests and demonstrations against DOD” ( p.i). More specifically, it found that CIFA analysts were not in violation of DOD directive 5200.27 that permitted gathering such information for law enforcement and force protection purposes. The report did find, however, that CIFA violated the 90-day retention rule specified by this same directive and that it “maintained TALON reports without determining whether information on organizations and individuals should be retained for law enforcement and force protection purposes” (p. ii). More specifically, of 1,131 reports examined by the IG that had been deleted from the CIFA Cornerstone database, 263 reports, or roughly 23 per cent, contained information on protests or demonstrations, and 334 reports, or roughly 30 per cent, contained information on U.S. persons.

On August 4, 2008, CIFA was officially “disestablished” while the “Defense Counterintelligence (CI) and Human Intelligence (HUMINT) Center” was simultaneously

activated. The stated purpose of this change was to more closely align “DoD CIFA and DIA HUMINT and CI functions.” So, although much of CIFA’s mission was retained by the new center, CIFA’s law enforcement function was not transferred, officially, at least, ending the CIFAs and more generally the DOD’s role in law enforcement (Aftergood, 2008).

In September, the DOD officially announced the closure of the “TALON reporting system” while noting that “intelligence oversight requirements” required the department to maintain copies of the data. While the Assistant Secretary of Defense for Homeland Defense and America’s Security Affairs worked on a replacement system, DOD personnel were directed to submit threat reports to the FBI’s Guardian reporting system (“DefenseLink News Release,” 2007).

What specifically has been shut down and for what reasons? This still isn’t entirely clear. The Cornerstone database, which CIFA used to maintain TALON reports, was officially shut down, but the data was retained. Further, the DOD spokesman who announced its decommissioning in August was careful to state that this was being done because the intelligence value had declined, not because of public pressure or criticism, and that it would be replaced (Burns, 2007). CIFA, though officially disestablished, had most of its functions absorbed by the new center. The only significant change seemed to be that the new center would not carry on CIFA’s mission for law enforcement. Threat data gathering would continue, however, and would now be funneled to a federal organization with full law enforcement authority, the FBI.

Rather than going away, the kind of reporting activity in the planned TIPS and the implemented TALON programs continues to grow rapidly. The remainder of this section describes SAR reporting as it stood late 2008 and early 2009, based on both official government documents (SORNS, PIAs, Inspector General Reports) and published investigative journalism.

Two particularly important documents, from which I will draw repeatedly, are: 1) the ISE-SAR functional standard document (version 1.0) issued by the Information Sharing Environment Program manager on October 24, 2008; and 2) the October, 2008 *Findings and Recommendations of the Suspicious Activity Report (SAR)* (hereafter, *Findings and Recommendations*), jointly published by the Department of Justice, Department of Homeland Security and the Major Cities Chiefs Association.

SARs are not simply collected; they are produced within very specific contexts which impact both the quality of the information and its potential subsequent usage. First, I will consider the primary SoRs where SARs are maintained and then examine both established and emerging institutional sites of production, from the FBI and military to the more than 800,000 local police departments and private sector, via the proto-institutions known as “fusion centers” and the InfraGard. Once I have considered these primary, emergent sites of production, I will look more closely at the logics of SARs, the how’s and why’s of their production. By examining the specific sites and generalized logics of report production we can better identify those aspects that make it problematic, that create dangers of more extreme SDS configurations.

## THE MAJOR SITES OF SAR PRODUCTION

### GUARDIAN SYSTEM

The two primary technological sites — physical systems of records — where the production of SARs takes place are the Guardian and E-Guardian systems maintained by the FBI. Access to the Guardian system is restricted to FBI agents and other authorized personnel, while the e-Guardian system is accessible to the broader state and local law enforcement community. A third system of records, the Tactical Information Sharing System (TISS), is maintained by the Federal Air Marshalls Service (FAMS) under the TSA. Reports in this system are called

Surveillance Detection Reports (SDRs) but they are simply another form of SAR. As I will explain more clearly within the logic section, all reports vetted and produced within these two institutions fall under the rubric of the overall ISE-SAR initiative.

In September, 2004, the FBI launched the Guardian system to “facilitate the accurate, complete, and timely reporting on the existence and status of terrorist threats.” The system, initially only available on the FBI’s intranet, collected reports from FBI agents and legal attaches, who were “required to enter ... new terrorism threats and suspicious incidents originating in their territory and use it to track resolution.” The FBI has reported that agents are expected to draw from multiple sources including: “(1) the general public, (2) other government agency partners, (3) state and local law enforcement, (4) ongoing FBI investigations and intelligence assessments, and (5) FBI Legal Attaches” (U.S. DOJ, 2008, November, p. 8). General threats and suspicious incidents make their way into agent reports via telephone calls, e-mail, mail correspondence, or through the FBI’s website. The Guardian system includes classified information up to the level of “secret.”

Over the course of 2005, more than 51,000 individual reports were entered into the system. By November of 2007, the database contained approximately 108,000 reports on “terrorism-related threats...suspicious activity or watch list encounters” (U.S. DOJ, 2008, November, p. ii). Not only had FBI been overwhelmed by the volume of data entered into the system, much of it was incomplete or inaccurate.

From our review of FBI database information, we determined that during fiscal year (FY) 2006, the public provided the FBI with approximately 219,000 tips that resulted in over 2,800 counterterrorism threats and suspicious incidents entered in Guardian for investigative follow up. (U.S. DOJ, 2008, November, pp. 8-9)

In the fall of 2008, the Guardian system was extended with a web-based component known as e-Guardian. Unlike Guardian, e-Guardian is restricted to unclassified information. E-

Guardian draws on a much larger field of people to produce SARs than does the Guardian system. According to the FBI, e-Guardian will be “available through our secure Law Enforcement Online Internet portal to more than 18,000 agencies, which will be able to run searches and input their own reports.” Data entered into the eGuardian database is immediately accessible at all fusion centers for vetting, where trained personnel decide whether the data will be retained and forwarded to the appropriate FBI task force or simply deleted from the system. According to an FBI web page, Guardian and eGuardian will “work together, feeding each other.”

eGuardian entries with a possible terrorism nexus will be pushed to Guardian and out to our task forces, and unclassified threat and suspicious activity information from the FBI housed in Guardian will be pushed to eGuardian and out to the entire law enforcement community. It’s an effective one-two punch. (“Connecting the Dots Using New FBI Technology,” 2008, n.p.)

Beauchamp, the FBI’s interim information technology portfolio manager at the Chief Information Officer’s Office in late 2007, explained that the eGuardian system was an attempt to “try to understand whether it is feasible to capture all suspicious activity data in a single repository or whether we need a distributed approach using Web services.” One thing that had already become clear by then was that, with over 120,000 users and continued expansion, the amount of data stored by the system was exploding (Miller, December 10, 2007).

The Center for Democracy & Technology (CDT), in their online blog, summarized the key problems associated with the FBI’s expanding threat reporting system:

The problems associated with the FBI’s Guardian system offer a glimpse of the challenges facing a huge new crop of data recipients under E-Guardian and the ISE. Both systems could exacerbate the data integrity problems of Guardian by encouraging state and local police to rely on fallible information. Before the new systems are made operational, the problems identified in Guardian need to be resolved. Effective oversight and data quality measures are crucial safeguards if civil liberties are to be meaningfully preserved in an era where government authorities regard intelligence gathering and sharing as the key to sound policing. (Geiger, 2008, n.p.)



While the FBI were the sole state agents responsible for entering and vetting suspicious activity reports within the Guardian system, the unclassified e-Guardian system connected more than 800,000 local police officers into the Department of Homeland Security's extended domestic intelligence network.

A pilot program at the LAPD developed a new training regime for officers to “gather, record, and analyze information of a criminal or non-criminal nature, that could indicate activity or intentions related to either foreign or domestic terrorism.” Among the types of behavior identified that would warrant SAR reports are taking pictures or video footage “with no apparent esthetic value,” taking notes, and “espousing extremist views.” Information generated by the police officers will be shared with their local fusion centers and from there to FBI SoRs Guardian and e-Guardian as well as information systems maintained by the DHS and other U.S. intelligence agencies (Sullivan, 2008). According to James Cohen, a senior advisor in the office of the Director of National Intelligence, the office is working with other federal agencies and state and local officials to “expand the Los Angeles model to 12 other cities and states, as part of a federal pilot program” (Gorman, 2008, n.p.).

On June 10, 2008, the Major Cities Chiefs Association, which as of June 2009 included 63 cities with populations over half a million, released a formal resolution endorsing the *Findings and Recommendations* and calling for the adoption of suspicious activity reporting practices in police departments nationwide (Major Cities Chiefs, 2008). According to the *Findings and Recommendations*, local police departments are advised to incorporate SAR reporting into their existing activities, for example, by simply adding a SAR checkbox to existing forms and paperwork.

Proponents of the program are quick to point out that much of what local police officers will do as part of the SAR initiative is simply sharing information they have already been creating. While this is true to a point, it is important to remember that the SAR initiative is not simply a new box to check on normal paperwork routines; it is also a mindset, a framing of suspicious activity heavily influenced by an episodic federal threat narrative, punctuated by threat assessments and other memoranda, issued by federal agencies and circulated amongst all participants in the Information Sharing Environment (ISE).

#### FUSION CENTERS

The fusion centers can be considered an extension of an initiative to “fuse” intelligence information that began with the establishment of the National JTTF in July, 2002. The National Joint Terrorism Task Force (NJTTF) and the now more than 100 local JTTFs in more than 100 cities nationwide have been the initial points of fusion for once “walled” intelligence agencies to share and analyze information. The NJTTF, as of 2004, consisted of 57 people from 38 U.S. agencies (law enforcement, intelligence, diplomatic, defense, public safety, and homeland security) (“A Closer Look,” 2004). Ken Love, Acting Chief of the NJTTF in July, 2004, describes its basic function:

It’s a pretty simple concept: we bring together people from every U.S. agency that collects and processes terrorist intelligence; we put them in one room and hook them into their own and into our FBI intelligence databases; and all of a sudden we have the universe of terrorist intelligence on the table — to share, to query, to coordinate, to answer questions, and to give direction and support to the 84 Joint Terrorism Task Forces (JTTFs) around the country that function under us. “Fusion” means that terrorist intelligence is instantly shared vertically from HQ to our JTTFs and horizontally to all NJTTF agencies. (“Meet the National Joint Terrorism Task Force,” 2004)

Local JTTF offices have been in existence since 1980, but they have grown in number and become much more important since the 9/11 attacks. A fusion center can be considered a more general class of the JTTF which involves state, local and private institutions as well. The

DOJ's official *Fusion Center Guidelines* describe the broad reach of data collection accompanying fusion center charters:

There is no single source for terrorism-related information. It can come through the efforts of the intelligence community; local, state, tribal, and federal law enforcement authorities; other government agencies (e.g., transportation and health departments); the private sector; and the general public. (U.S. DOJ, n.d., p. 11)

Although some fusion centers were in operation before the 911 attacks, they were not widely deployed nationally until early 2005. In December, 2004 the President's Homeland Security Advisory Council recommended "each State should establish an information center that serves as a 24/7 'all-source,' multi-disciplinary, information fusion center" (U.S. DHS, 2005, p. 4). Between 2004 and 2007, the Department of Homeland Security dispersed \$254 million in support of the centers, while the FBI and other federal law enforcement agencies have personnel on site. Fusion centers are generally led by local law enforcement chapters such as the state police or the FBI, but also regularly work with DOD personnel and the U.S. Northern Command. Because fusion centers are officially administered by state, not federal government, they are not subject to federal privacy laws and have developed in different ways. Although most early fusion centers began with a focus on counter-terrorism, the role of fusion centers has tended to expand over time to a broader orientation toward general criminality. Los Angeles Police Chief William Bratton, in a 2008 speech to the National Fusion Center Conference in San Francisco, explained the reasoning for this ongoing transformation:

Now, let's address the ongoing debate over whether fusion centers should be strictly designed to counter terrorism or whether they should address "all crimes, all hazards."

To advocate the position that fusion centers should be strictly designed around terrorism demonstrates a complete lack of understanding of the public safety risk, threat matrices, and the need to engage the majority of local law enforcement. It also demonstrates a complete lack of understanding about how terrorists are recruited, how terrorists plan and execute their operations and the criminal markets that support terrorist organizations.

The idea of terrorism has come a long way since the days of the Red Brigades. Al Qaeda, FARC and other groups have been successful at exploiting the vulnerabilities of their

enemies. In our case, they attacked the arrogance and turf battles that were at the heart of our failure to communicate. As we heard Secretary Chertoff say in this forum last year: “We have to build a network to beat a network.” That is precisely what we will do.

My position on the role and operation of fusion centers has been adopted by all the chiefs from America’s large cities - intelligence must be gathered on all crimes and fully integrated into the daily operations of the police department. In our view, intelligence should inform and shape the wide range of police services that protect the public. For example, it is critical that we receive timely threat intelligence from the federal government so that we can determine what measures may be taken by police and emergency service agencies (Bratton, 2008, March 19, n.p.).

According to the GAO, 43 fusion centers were operational nationwide by September 2007, 34 of which had opened since January, 2004 (U.S. GAO, 2007, October). Fusion centers have access to a range of public and private information systems. Most working centers have access to unclassified networks such as the Homeland Security Information Network (HSIN) and Law Enforcement Online (LEO). Most have commercial accounts with data aggregators such as Choicepoint, Accurint and Lexis/Nexis. In addition, roughly half of the centers indicated they were in the process of gaining access to classified DHS and FBI networks and other federal data systems (“Centers Tap into Personal Databases,” 2008).

Although the role of fusion centers in sharing and distributing information has been heavily emphasized, it must not be forgotten that they also play a significant role in producing information, including PII. For example, the *Denver Post* reported in the summer of 2008 that fusion centers across the country were beginning to deploy Terrorism Liaison Officers (TLOs) to generate reports of suspicious activity within their communities. In Colorado, as of July, 2008, 181 police, firefighters, paramedics and even utility workers had been trained and were deployed after FBI-led training (Finley, 2008). *Progressive* reporter Mathew Rothschild, who located a TLO position announced for East Bay, San Francisco, noted that in addition to locations around the waterfront, TLOs might be situated on the campuses of universities (Rothschild, 2008a).

TLOs report to FBI representatives at their local fusion center. Information provided may then be written into a formal SAR report, based on the agent's judgment.

A major concern about the Fusion Centers raised by privacy groups such as EPIC is the way in which they appear to fall through the cracks of the country's legal infrastructure for privacy protection. Although the DOJ's guidelines on fusion centers include a section on privacy and civil liberties, and fusion centers are recommended to follow the principles of Fair Information Practices, these are voluntary guidelines, not legal mandates. EPIC has called for formal oversight of fusion centers ("National Network' of Fusion Centers," 2007).

#### INFRA GARD

An increasing number of private sector professionals are being recruited to serve as additional channels of domestic intelligence production in the FBI-sponsored InfraGard program. The ACLU has compared the program to Ashcroft's TIPS program:

"There is evidence that InfraGard may be closer to a corporate TIPS program, turning private-sector corporations-some of which may be in a position to observe the activities of millions of individual customers-into surrogate eyes and ears for the FBI," (Stanley, 2004, p. 12)

First formed in Cleveland in 1996, the FBI made and promoted a national template for the program in January, 2001. By March, 518 companies, including Coca-Cola and Delta, had joined the program. By November of that year, InfraGard totaled 1700 members. Total membership exceeded 23,000 members by January 2008 (Rothschild, 2008b). An FBI web page describes the program:

It's the twenty-first century: a globalized, systems-driven, networked age. Our job is to prevent attacks-both physical and electronic-against critical infrastructure: banks ... hospitals ... telecommunications systems ... emergency services ... water and food supplies ... the Internet ... transportation networks ... postal services ... and other major industries that have a profound impact on our lives.

Precisely the point of an eight-year-old alliance between the FBI and the public called InfraGard. Our program has over 14,800 private sector members spread across 84 local chapters nationwide. That's more than the total number of FBI Agents.

These partners represent the full sweep of infrastructure experts in local communities: business executives, entrepreneurs, military and government officials, computer security professionals, academia, state and local law enforcement, and any concerned citizens.

The essence of the partnership is information and intelligence sharing. FBI Agents assigned to each chapter bring meaningful news and information to the table: threat alerts and warnings, vulnerabilities, investigative updates, overall threat assessments, case studies, and more. Our private sector partners—who own and operate some 85 percent of the nation's critical infrastructures—share expertise, strategies, and most importantly, leads and information that help us track down criminals and terrorists. (“InfraGard: FBI and Private Sector,” 2008, n.p.)

InfraGard members can share information via a secure, exclusive network or in person during special meetings and seminars. Members of the InfraGard are trained to supply raw suspicious activity reports to their FBI contacts, who may then enter this information into a threat reporting system such as Guardian as a formal SAR. InfraGard members are given legal immunity for information that they choose to supply (Rothschild, 2008b) and, in return, may be rewarded with insider information that even high level government officials may not have access too.

On November 1, 2001, the FBI had information about a potential threat to the bridges of California. The alert went out to the InfraGard membership. Enron was notified, and so, too, was Barry Davis, who worked for Morgan Stanley. He notified his brother Gray, the governor of California.

“He said his brother talked to him before the FBI,” recalls Steve Maviglio, who was Davis's press secretary at the time. “And the governor got a lot of grief for releasing the information. In his defense, he said, ‘I was on the phone with my brother, who is an investment banker. And if he knows, why shouldn't the public know?’” (Rothschild, 2008b)

## THE LOGIC OF SAR PRODUCTION

### THE INFORMATION SHARING ENVIRONMENT (ISE)

The Information Sharing Environment (ISE) is the most general logic under which the SAR program operates. The 9/11 Commission found that a lack of information sharing between

agencies like the CIA and FBI was one of the primary reasons U.S. intelligence failed to identify and mitigate the 9/11 conspiracy. As discussed in Chapter 3, Section 1016 of IRTPA (2004) called for the creation of an Information Sharing Environment (ISE) and defined it as “an approach that facilitates the sharing of terrorism information.” The law called for the President to designate a Program Manager for the ISE (PM-ISE) and establish an Information Sharing Council to advise the President and the Program Manager. The council includes members from the Department of Commerce, the Central Intelligence Agency, Department of Defense, Director of National Intelligence, Federal Bureau of Investigation, Department of Homeland Security, National Counter Terrorism Center, and many other departments with connections to national security.

The PM-ISE lays out the vision of the ISE in its implementation plan:

We envision a future ISE that represents a trusted partnership among all levels of government in the United States, the private sector, and our foreign partners, to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism against the territory, people, and interests of the United States of America. (McNamara, 2006, p. xiii)

As of June 2009, the first two priorities listed for the PM-ISE office were the establishment of fusion centers nationwide and the institutionalization of a Suspicious Activity Reporting framework.<sup>30</sup> This framework is documented within the ISE-SAR standard and the *Findings and Recommendations*.

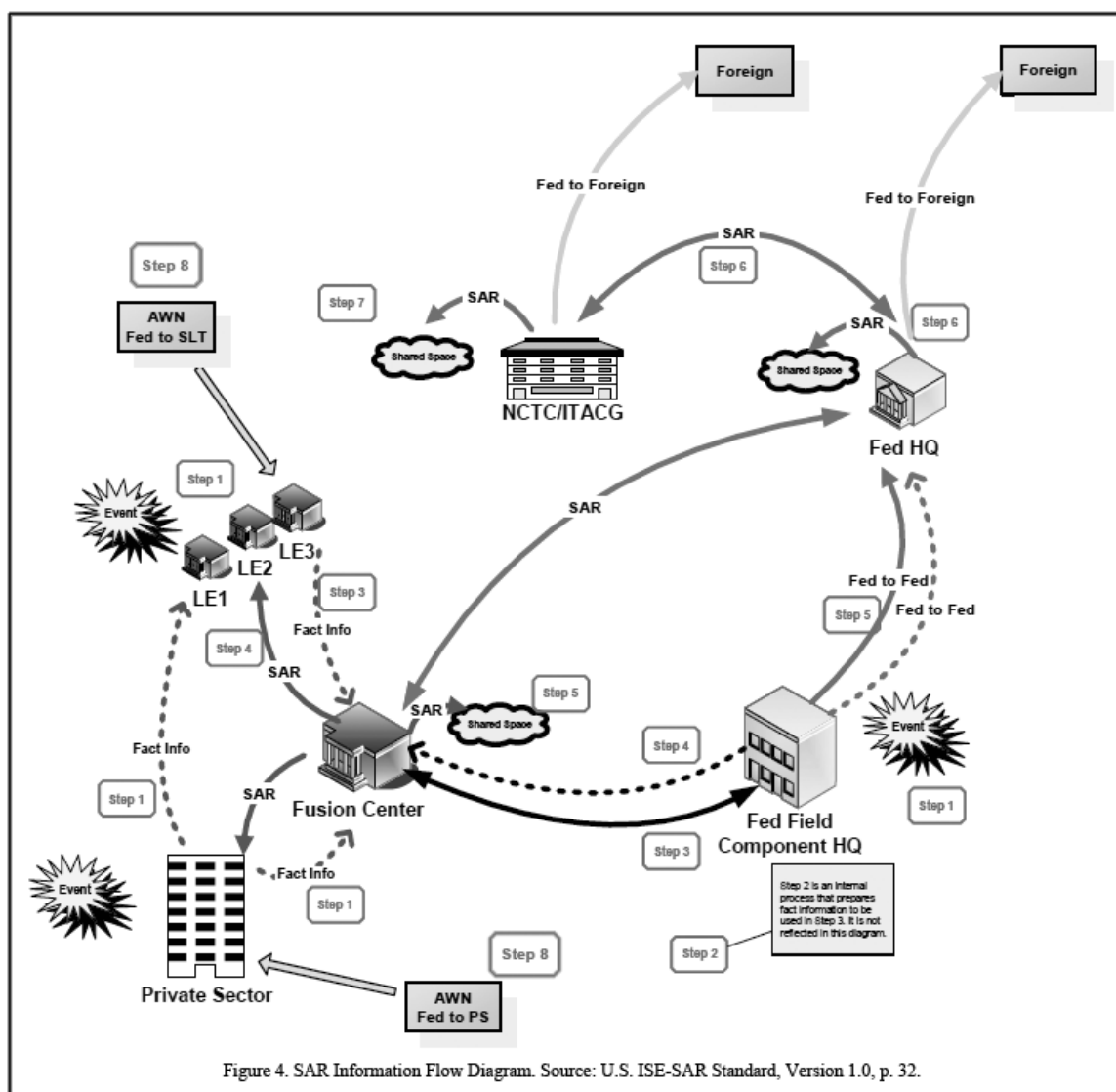
#### THE SAR PRODUCTION AND SHARING PROCESS

The information acquisition process for SARs occurs via multiple vectors, including on-duty police officers, telephone tip lines, and active military personnel. Before a general report of suspicious activity can be turned into an official ISE-SAR it must be first vetted within the receiving organization. This front line organization could be anything from a small local police

---

<sup>30</sup>Ise.gov web site, retrieved 6/11/2009 from <http://www.ise.gov/pages/vision.html>.

office to a major city police precinct to a state fusion center. The rigor and expertise involved in the initial evaluation depends in part on where the initial report is received. If it is in a small police department, it is quite likely that the initial determination of terrorism connection will be made by someone without formal counterterrorism training. This officer will have seen a recent “threat assessment” published by the Interagency Threat Assessment and Coordination Group



(ITACG) located at the NCTC (“Interagency Threat Assessment and Coordination Group,” n.d.) or literature produced by his regional fusion center which helps her to make this determination.



Assuming the local police agency decides a report qualifies as a SAR, they submit it to their local fusion center. If the agent decides it does not warrant forwarding, what happens to the report at this time depends solely on local policies regarding general SAR reports. Surveillance detection reports produced by Federal Air Marshals are stored within the Tactical Information Sharing System (TISS) for a period of 25 years. SARs produced and stored by local police departments are generally retained for up to 5 years. DOD TALON reports, SARs that were the subject of scandal in 2005-6 for reporting peace marches as threats, were supposed to be deleted from the reporting system within 90s days, but remained long after (U.S. DOD, 2007, June 27).

At the fusion center, a trained agent evaluates incoming raw SAR reports. If the report is determined to be terrorism-related, the fusion center agent then places the report into the ISE-SAR format and stores it within the "ISE Shared Environment." The ISE Shared Environment is a dedicated server that is networked with all other fusion centers, JTTFs and the FBI's E-Guardian network. Depending on the seriousness of the report, it may also be forwarded directly to counterterrorism institutions such as the JTTF. This record then becomes instantly accessible to (searchable by) all fusion centers, while remaining in control of the originating fusion center or other participating, authorized ISE-SAR institution.

According to this official U.S. ISE SAR standard, there are only two situational categories that should lead to the production of a SAR: 1) intelligence gathering and 2) pre-operational planning. Although at first glance this may appear to be a narrow enough definition to insure that moments of SAR production are limited to reduce the noise factor and preserve civil liberties, this definition is being extended in both practice and policy. In the past decade, we already have historical examples of SAR reporting programs exceeding their mandate and producing reports on First Amendment activity. Even the current *Findings and Recommendations*, jointly released by the Department of Justice, Global Justice Information

Sharing Initiative and the Department of Homeland Security, cautions that the current ISE standard offers too narrow a definition and recommends that the ISE “update the common definition for suspicious activity:”

... the suspicious activity may be an actual attack or other crime. It may be a report of a suspicious association or material that supports activity. Because of these limitations, consideration should be given to expanding the definition: “Reported or observed activity and/or behavior that, based on an officers training and experience, is believed to be indicative of criminal activity associated with terrorism” (pp. 3-4).

There is further guidance on behavior that might fit the profile for an SAR in *Appendix C* of the ISE-SAR standard document. Among other triggers, it identifies *surveillance*, the “Monitoring the activity of people, facilities, processes or systems,”; *Expressed or Implied Threat*, “Communicating a spoken or written threat to damage or compromise a facility/infrastructure,”; *Acquisition Of Expertise*, “Attempts to obtain or conduct training in security concepts, military weapons or tactics, or other, unusual, capabilities, such as specialized transport or handling capabilities”; *Sector-Specific Incident*, “Actions associated with a characteristic of unique concern to specific sectors (such as the public health sector), with regard to their personnel, facilities, systems or functions”; *Recruiting*, “Building of operations teams and contacts, personnel data, banking data or travel data,” and *other*, “Incidents not in above categories.”

In early 2008, the Office of the Director of National Intelligence issued standards for Suspicious Activity Reports (SARs) that are to be shared across the national ISE (U.S. DNI, 2008, January 28). Information that is “personally identifiable” is tagged with a privacy flag, so that it can be easily removed to produce an anonymized SAR. The ISE-SARs document tags particular types of data as “privacy fields” that must be removed before a SAR qualifies as a “Summary-SAR,” the “anonymized” version of the “Detailed-SAR.” While the standards require that first and last names and driver’s license numbers be removed, the “anonymized” record can

retain the subject's birth date, height and weight, as well as the state of issue, issue date and expiration date of their driver's license. With these remaining non-privacy fields, reconstructing the identity of the SAR subject is a trivial matter.

#### SAR PRODUCTION TRIGGERS

The SAR standard contains much language stressing the flexibility local institutions have in defining what constitutes suspicious activity. In the *Findings and Recommendations*, local fusion centers and policing agencies are advised to develop and circulate literature that helps people to understand what constitutes suspicious activity. The logics that trigger SAR production can have little to do with rational concerns about international terrorism, however, as the following two examples help illustrate.

An investigative report by Tony Kovaleski of the Denver television station KMGH found that Federal Air Marshals in Las Vegas Nevada were regularly generating false Surveillance Detection Reports (SDRs) simply to meet quotas set by the managers, with the impression that the quota “directly reflects on (their) performance evaluations” and on “how much money they make.” The reporter found a department memo, dated July, 2004, which said “[t]here may come an occasion when you just don't see anything out of the ordinary for a month at a time, but I'm sure that if you are looking for it, you'll see something.” Air Marshals interviewed in the course of investigation identified specific instances when innocent air travelers had their names entered into a report just to meet quotas:

“To meet this quota, to get their raises, do you think federal air marshals in Las Vegas are making some of this stuff up?” Kovaleski asked.

“I know they are. It's a joke,” an air marshal replied.

“Have marshals in the Las Vegas office, I don't want to say fabricated, but ‘created’ reports?” Kovaleski asked.

“Creative writing — stretching a long ways the truth, yes,” an air marshal replied.

One example, according to air marshals, occurred on one flight leaving Las Vegas, when an unknowing passenger, most likely a tourist, was identified in an SDR for doing nothing more than taking a photo of the Las Vegas skyline as his plane rolled down the runway.

“You’re saying that was not an accurate portrayal of a potential terrorist activity?” Kovalski asked.

“No, it was not,” an air marshal said. (“Marshals: Innocent People,” 2006, n.p.)

Don Strange, a former agent in charge of Air marshals in Atlanta, warned that the repercussions for someone falsely placed on such a report could be severe: “[t]hat could have serious impact ... They could be placed on a watch list. They could wind up on databases that identify them as potential terrorists or a threat to an aircraft. It could be very serious” (“Marshals: Innocent People,” 2006, n.p.).

In early 2009, a conspiracy-oriented website headed by Austin radio and public access personality Alex Jones, Infowars.com, released copies of an internal memo distributed by the Missouri Information and Analysis Center (MIAC) and the Missouri State Highway Patrol entitled, “The Modern Militia Movement.” The document presented a narrative of the rise, fall and return to prominence of a terrorist militia movement characterized by white supremacy, fear of a “New World Order” and interest in third party candidates including Ron Paul and Bob Barr.

Academics contend that female and minority empowerment in the 1970s and 1960s caused a blow to white male’s sense of empowerment. This, combined with a sense of defeat from the Vietnam war, increased levels of immigration, and unemployment, spawned a paramilitary culture. This caught on in the 1980’s with injects such as Tom Clancy novels, Soldier of Fortune Magazine, and movies such as Rambo that glorified combat. This culture glorified white males and portrayed them as morally upright heroes who were mentally and physically tough.

It was during this timeframe that many individuals and organizations began to concoct conspiracy theories to explain their misfortunes. These theories varied but almost always involved a globalist dictatorship the “New World Order (NWO),” which conspired to exploit the working class citizens. United States troops were thought to already be operating in the U.S. in support of the NWO. Much of this rhetoric would become anti-semitic claiming that Jews controlled the monetary system and the media.... (p. 1)

Political Paraphernalia: Militia members most commonly associated with 3<sup>rd</sup> party political groups. It is not uncommon for militia members to display Constitutional Party, Campaign for Liberty, or Libertarian material. These members are usually supporters of former Presidential Candidate: Ron Paul, Chuck Baldwin and Bob Barr.

Anti-Government Propaganda: Militia members commonly display picture, cartoons, bumper stickers that contain anti-government rhetoric. Most of this material will depict the FRS, IRS, FBI, ATF, CIA, UN, Law Enforcement and “The New World Order” in a derogatory manner. Additionally, Racial, anti-immigration, and anti-abortion, material may be displayed by militia members. (p. 8)<sup>31</sup>

Shortly after the report was circulated online, it became a large enough topic of public interest to require a response from the state of Missouri. On March 25, 2009, Lt. Gov. Peter Kinder called for Department of Public Safety Director John Britt to be placed on leave because of the report. Britt apologized for the “political profiling” and promised to take it immediately out of circulation. Defending Britt, Col. James Keathley of the Missouri Highway Patrol stated that the report was circulated to Missouri policeman without being properly vetted by himself or Britt and that the “flawed oversight system” needed to be revamped (Moring, 2009).

While this material is only from one state, its contents suggest that in at least some states the eyes and ears of domestic intelligence are being trained to view those with marginal political views and dissidents as potential members of the militia movement and therefore potential terrorists. Given the excesses that have occurred in the past, it seems likely that this kind of training material, if widely circulated, will lead to the generation of SAR reports on Americans whose only “crime” is the exercise of their First Amendment right to speak out in criticism of their government.

#### WATCH LISTS

In the years since September 11<sup>th</sup>, significant public attention has been paid to the government’s plan to expand, update and improve a watch list program to keep potentially

---

<sup>31</sup> Copy of complete report retrieved 8/15/2009 from <http://www.constitution.org/abus/le/miac-strategic-report.pdf>

dangerous terrorists out of the airline system. The Computer Assisted Passenger Pre-Screening system (CAPPS) was first launched in 1998 after the crash of TWA Flight 800, as part of a package of new security measures installed at airports. The system, in its original form, flagged suspect travelers for extra scrutiny from security, but did not, in and of itself, produce decisions about whether an individual could get on a plane. On September 11<sup>th</sup>, six of the eighteen hijackers were flagged by the system for extra security, for the gate inspectors to check their luggage more thoroughly or pat them down for weapons. According to the 9/11 Commission Report, all six of these flagged passengers eventually boarded the planes that day.

The controversy and legal struggles over this updated watch list program provide an important example of a key SDS tool and the effectiveness of organized public resistance. Before looking at this struggle in more detail, across three nominally different systems — CAPPS II, Secure Flight and the Automated Targeting System (ATS) — it is important to consider the watch list in historical context. Rather than being announced in the form of a Systems of Records Notice (SORN) or Privacy Impact Assessment (PIA), the FBI's watch list program from the 1920s to the early 70s was exposed in the Church Committee hearings.

#### HISTORICAL CONTEXT: HOOVER'S WATCH LISTS

Between 1919 and 1921, J Edgar Hoover, before becoming director of the FBI, led a series of large-scale nationwide arrests called the Palmer Raids, named for then Attorney General Mitchell Palmer. Armed with a list of more than 150,000 names, from late 1919 to 1921 FBI agents violently apprehended and took into custody anarchists and anti-war advocates they believed to be responsible or “fellow travelers” with those who plotted violent overthrow of the government. The raids had followed a series of bombings attributed to these violent anarchists, including twice at the AG's residence. The Palmer raids still stand as the largest mass arrest in U.S. history, with over 10,000 individuals apprehended and arrested. Though these raids would

be soon condemned within the public eye and by the new President and Attorney General, the practice of keeping lists was continued and expanded by Hoover as director of the FBI.

During Hoover's tenure at the FBI, the bureau maintained a watch list originally known as the "Custodial Detention List." Candidates for inclusion on the list, begun in 1939, were described as having communist "tendencies" or being "communistic." In 1941, criteria were expanded to include "pronouncedly pro-Japanese" individuals. Those on the list were candidates for immediate arrest and imprisonment in the event of a national emergency. In 1943, then Attorney General Francis Biddle, noting the absence of any Congressional authorization for the list, ordered its termination. Hoover, ignoring the AG's directive, simply renamed the detention list to "Security Index" and continued its operation (Donohoe, 2006).

In 1950, with the passage of the Internal Security Act, the "security index" gained partial legal status. The emergency detention provisions of the Act gave the government the authority to round up and indefinitely detain dissidents without trial, based on the simple assertion by the Attorney General that they would "probably" engage in future illegal conduct. In addition to the "security index," another, larger list called the "reserve list" named people who would be subject to "priority investigation" after the arrests of persons on the "security index." Names on the lists included "educators, labor union organizers, lawyers, doctors and scientists" and "individuals who could potentially furnish financial or material aid" to an enemy (Goldstein, 2001, p. 324). According to one former FBI agent, the combined lists, at their peak, contained more than 500,000 names (Swearingen, 1995).

In 1971, with its repeal of the "Emergency Detention Provisions of the Internal Security Act of 1950," Congress outlawed the "security index" program. Rather than dissolve the program

outright, Hoover simply changed its name again, this time to the “Administrative Index” or ADEX.

Attorney General Mitchell approved the FBI’s decision to keep an “administrative index” on the grounds that the authority to create a list compiled and maintained to assist the Bureau in making readily retrievable and available the results of its investigations into subversive materials and related matters is not prohibited by Repeal of the Emergency Detention Act. While the FBI did not tell Mitchell explicitly that the ADEX would also serve as an emergency arrest list in asking for his approval, according to a Senate Intelligence Committee staff report, there was “informal” Justice Department knowledge of the real purpose of the list. (Goldstein, 2001, p. 439)

The ADEX combined the Security and Reserve Indices, with Reserve names making up the lowest priority category. The minimal criteria for inclusion on the ADEX was that an individual be “in a position to influence others to engage in acts inimical to the national defense or furnish financial aid or other assistance to revolutionary elements because of their sympathy, associations, or ideology.” Church Committee hearings in 1976 uncovered the existence of the ADEX list and ordered its termination. Though official documentation is lacking, there is evidence that administration of the ADEX list then shifted from the FBI to FEMA as part of its Continuity of Government (COG) program (Dubose, 1987; Sklar, 1988).

Watch lists can be considered the ultimate reduction of an individual’s state dossier system information into a binary categorization: absence/presence. Presence on a particular list is a signal for a state agent to act on the listed subject in a particular way. As with the original CAPPS list, this action might simply involve increased attention and screening. Today it might involve being denied boarding of a particular flight, being immediately apprehended and incarcerated, or being denied a job.

Due to the potential power of the watch list, potential listees and the public at large clearly have an interest in knowing the logic of a particular watch list’s production. What are the factors that determine whether a particular person is on this or that list? What sources of



information contribute to this calculation? Because of national security concerns, state officials are naturally reluctant to make this process transparent. At the same time, without the ability of a listee to understand and/or challenge the reasons for his/her listing, it creates a particularly problematic interface between the state and the subject.

Since the September 11<sup>th</sup> Attacks, the idea of watch lists has been particularly salient in debates over the emerging surveillance society. Three lists in particular — the consolidated terrorist list, the no fly list, and the selectee list — have gotten significant attention from the public. These lists are connected with a series of government programs to enhance the security of airline travel.

#### CAPPS, SECURE FLIGHT, ATS

CAPPS II, originally scheduled to be launched in 2004, was intended to upgrade the existing watch list system in two major areas. First, it was slated to draw on a much higher volume of data (including private data) to make its risk assessments. Second, the system added a higher degree passenger risk assessment that, if assigned to a particular traveler, would be enough to forbid them from boarding the plane (but not necessarily to be taken into custody).

On January 15, 2003, the Department of Transportation, then the home department for the TSA, issued a SORN describing an Aviation Security Screening Records (ASSR) system. Although, the term CAPPS was not used in this original SORN, all subsequent references to the system by the TSA would use the term CAPPS II. According to the SORN, the system would be used “to facilitate the conduct of an aviation security-screening program, including risk assessments to ensure aviation security.” The new risk assessment for CAPPS II marked the first introduction of a color-coded system in which travelers would be assigned one of three colors

(green, yellow, red) indicating their relative degree of risk. To make this determination, a wide range of public and private data would be used:

Passenger Name Records (PNRs) and associated data; reservation and manifest information of passenger carriers and, in the case of individuals who are deemed to pose a possible risk to transportation security, record categories may include: risk assessment reports; financial and transactional data; public source information; proprietary data; and information from law enforcement and intelligence sources. (68 FR 45265, August 1)

Data maintained within the CAPPs II, as outlined in the SORN, could be disclosed to a wide range of public and private entities, from private contractors and individuals to agents of government, both domestic and foreign, whenever TSA “becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.” Individuals that TSA deems to be a threat to aviation security would have their information retained for up to 50 years. The DOT announced an effective date for CAPPs II of February 24, 2003. If no comments or criticisms were submitted by that date, the CAPPs II system as described in the SORN would be implemented. If comments were received, the DOT would issue a new, revised SORN designed to address these comments and criticisms.

The broad coverage and scope of the CAPPs II system as it was announced in January drew harsh criticism from the public at large, from newspaper reporters to privacy activists to members of Congress.

there are ... serious questions surrounding law enforcement access to data held by multiple commercial data providers and whether that access might just be an end run around the Privacy Act.... Additionally, part of the purpose behind the Privacy Act was to ensure that information the government did collect about individuals was accurate. The poor quality of data in the various commercial databases such as credit reports has been well documented. There is a significant possibility that the use of multiple-source commercial databases would result in a number of incorrect determinations because of the bad data stored in these databases — garbage in, garbage out. (“EPIC Comments on the TSA,” 2003)

The only difference between the TIA [Terrorism Information Awareness] program and the Department’s current proposals is that the ASSR system would, at least nominally, be

limited to those who travel at some time by air. Given the prevalence of air travel in the USA, that is not a very significant limitation or distinction. (Hasbrouck, 2003, n.p.)

In response to criticism, the TSA, now under the DHS, released its revised SORN for the CAPPS II system. The revised description, which Hasbrouck (2003) dubbed CAPPS 2.1, significantly limited the amount of private data to be used by the system. According to the SORN issued on August 1, 2003, the Passenger Name Record (PNR) would be the only commercial data submitted to the CAPPS II system.

The change in flight reservation procedures under CAPPS II required passengers to provide four pieces of information to the ticketing agent when making their reservation: full name, home address, phone number and date of birth. This data would be entered into the PNR, which would then be sent electronically to CAPPS II. Sometime later, prior to the flight date, the CAPPS II system would send the information in the PNR to commercial contractors for the purpose of verifying the passenger's identity:

The CAPPS II system will access PNRs prior to the departure of the passenger's flight. Selected information will be securely transmitted to commercial data providers, for the sole purpose of authenticating passenger identity. This authentication will be accomplished not by a permanent co-mingling of data, but merely by the commercial data providers transmitting back to TSA a numeric score, which is an indication of the percentage of accuracy of the match between the commercial data and the data held by TSA. This will enable TSA to have a reasonable degree of confidence that each passenger is who he or she claims to be. (68 Fed. Reg. 45265, August 1, 2003)

Risk determinations would not use private data. After obtaining the numeric identity verification score from the commercial partner, CAPPS II would perform its risk assessment using government databases, including classified and intelligence data, leading to one of three assessments: acceptable risk, unknown risk, or unacceptable risk. This assessment would then be transmitted to the air carrier, so that, at check-in, the proper action could be carried out, ranging from allowing the individual to board the plane after passing through standard gate procedures, to law enforcement taking him or her into custody.

Although representatives of the TSA argued that this PNR data was already being produced by the airlines, the reality was far different. According to a March 15, 2004 working paper presented by the International Air Transport Association (IATA) for the session of the International Civil Aviation Organization's "Facilitation Division" later that month in Cairo, Egypt, not only was the PNR data not already available, but meeting TSA's requirements could involve industry restructuring costing in excess of U.S. \$2 billion:

Since only portions of Airline Reservation Systems are regulated by Industry standards, significant parts of the underlying architecture vary. Any movement to impose changes on the industry with respect to the way that PNR's are constructed, stored or exchanged would require a massive restructure of the entire industry's underlying IT base. While no firm analysis has been undertaken to identify the final cost of such a restructuring across the industry — including within the Travel Agency community — some in the industry have estimated that the costs could conceivably exceed U.S. \$2 billion. ("Airline Reservation System," 2004)

As several privacy activists subsequently pointed out, even the revised CAPPS II system had significant violations of privacy built into its design, particularly in the way it would create legal requirements for the production of dossier data that would then be maintained, free of federal privacy laws, by private companies:

The additional information required by CAPPS 2.1 could be used to correlate each travel reservation (currently indexed only by flight number or reservation record locator) with a specific person, and to index separate reservations for individual trips into databases easily searchable by name, birthday, address, or phone number. CAPPS-II would thus enable the government and private travel companies ... to create comprehensive lifelong dossiers of everywhere each person has travelled, when, how, with whom, whether (behind the closed doors of their hotel room) they asked for one bed or two, and many other intimate details of their lives as revealed by their travel histories. (Hasbrouck, 2004)

Further, despite the TSA statement that it would not retain data on most Americans once their flights were completed, there are no comprehensive privacy laws that would prevent the TSAs private contractors from maintaining this information and even selling it back to the government at a later date. In addition, the revised CAPPS II system continued to include a scope beyond purely identifying terrorists to include "serious violations of criminal law."

On October 1, 2003, President George W. Bush signed Department of Homeland Security Appropriations Act, 2004 (HR 2555), which contained language specifically prohibiting the use of funds for the CAPPs II system until the full review by the General Accounting Office determined the program had met eight specific criteria, including “a system of due process” for people to appeal their listing and “correct erroneous information,” a low number of false positives, the establishment of an internal oversight board and the establishment of satisfactory privacy and security measures. Despite the clear cut language of the bill, Bush issued a signing statement declaring that while the bill’s language was mandatory, he would construe it as “merely advisory” (“Homeland Security Appropriations,” 2008, n.p.).

In August 2004, the DHS announced that the CAPPs II plan would be terminated, and a new initiative, Secure Flight, developed in its place. Secure Flight was supposed to address some of the key criticisms. For example, Secure Flight would seek only to identify terrorists, not suspected violent criminals. The red, yellow, and green colored threat designations were done away with, though the underlying three part risk categorization remained. Commercial data would no longer be used to determine a passengers risk factor, although it would be used for initial identify verification. Risk designation would be determined by the TSA in consultation with the TSC. Finally, the new Secure Flight included a new system for passenger redress, to correct situations in which innocents inadvertently appeared on the list.

A key aspect to understand about the creation and use of a watch list is the act of actually matching a name on the list to a person standing before the agent. As names are not true indexical identifiers, it is entirely possible for more than one person to have the same name, or a single person to engage in transactions where the spelling of his or her name varies due to human error or other reasons. From the state perspective, failing to match a terrorist to the list when they are standing before an agent could greatly endanger the air system. From a passenger’s point of

view, wrongly being matched to a list would likely inconvenience them or have a major impact on their life. In 2005 and 2006, major media outlets featured stories of individuals with common names like “David Nelson” whose lives had been disrupted by frequent missed flights and mistreatment by authorities. Also, from the state’s perspective, too many such “false positives” will clog the system and reduce the likelihood that real threats will be spotted. For this reason, there is a recognized need on both sides to improve the process by which names are matched to watch lists. One of the ways to reduce this occurrence, argued the TSA, was to take away this responsibility from the airlines and give it directly to the TSA.

Despite these changes, privacy and human rights NGOs remained firmly against the program in principle, and pointed out that the new requirements for airlines to submit Passenger Name Records (PNRs) with specific data fields also opened the door to airlines maintaining private travel dossiers that they could then sell back to the government at a later date. In February, 2006, the GAO released a highly critical report of Secure Flight, noting the apparent lack of oversight the program and numerous security and hardware vulnerabilities. The GAO also noted major gaps in the information provided to them concerning where personal data would come from and how it would be handled.

By the end of the year, critics began to wonder if the reason Secure Flight appeared to be in such disarray was that its proposed functions were already largely being met by a system already in place, one focused only on international travel, but that had not been publicly vetted in the way that CAPPS II and Secure Flight were:

ATS is an Intranet-based enforcement and decision support tool that is the cornerstone for all CBP [Customs Border Patrol] targeting efforts. CBP uses ATS to improve the collection, use, analysis, and dissemination of information that is gathered for the primary purpose of targeting, identifying, and preventing potential terrorists and terrorist weapons from entering the United States. Additionally, ATS is utilized by CBP to identify other violations of U.S. laws that are enforced by CBP. In this way, ATS allows CBP officers

to focus their efforts on travelers and cargo shipments that most warrant greater scrutiny. ATS standardizes names, addresses, conveyance names, and similar data so these data elements can be more easily associated with other business data and personal information to form a more complete picture of a traveler, import, or export in context with previous behavior of the parties involved. Every traveler and all shipments are processed through ATS, and are subject to a real-time rule based evaluation. (71 FR 64543, 2006)

This Systems of Records Notice (SORN), published on November 22, 2006, was the cause of considerable controversy. The ATS system, as described in the SORN, appeared to fit within the definition of watch list programs forbidden by Congress until specific conditions had been met. Now, the TSA was suggesting that such a system had been running all along, since 1998, and that its activities were covered by the SORN for an existing system, the Treasury Enforcement Communications System (TECS), of which ATS was only one module. Although ATS differed from Secure Flight in that it focused only on international travel, both systems required airlines to submit PNR records and both relied on general watch list data provided by the Terrorist Screening Center. In addition to drawing information from commercial databases (the PNRs), ATS was recording details about passenger dispositions as they interacted with Customs Border Patrol (CBP) agents.

“Clearly the law prohibits testing or development” of such computer programs, said Rep. Martin O. Sabo (D-Minn.), who wrote the three-year-old prohibition into homeland security funding legislation. “And if they are saying that they just took some system, used it and therefore did not test or develop it, they clearly were not upfront about saying it.” (Nakashima & Hsu, 2006)

The ACLU similarly decried the move:

“The government tried to institute the CAPPS II program of ‘risk assessments’ on passengers several years ago, and a huge uproar rightly followed, and the Congress was forced to intervene,” said Steinhardt. “We are stunned to learn that DHS is now implementing an even more far-reaching program with virtually no opportunity for the public to evaluate or comment on it.” (Government Secretly Tracks, 2006, n.p.)

Neither the ATS nor the proposed Secure Flight systems rely directly on private sector contractors to calculate risk ratings. Rather, they rely on lists maintained by the Terrorist Screening Center and, in the case of Secure Flight, by the TSA as well. Although the government

does not release data on the specifics of who is on these lists or how they are generated, it does periodically provide general numbers. As press reports have often tended to focus on the large size of some of these measures, there has been considerable confusion about just what government lists are being talked about. For the purposes of this discussion, it is useful to distinguish between three lists: the “comprehensive terrorist list,” the no fly list, and the selectee list. Below, a 2008 GAO report distinguishes between the no fly list and the larger selectee list:

TSA outlines air carrier requirements in the No Fly List Procedures security directive, requiring domestic air carriers to conduct checks of passenger information against the No Fly List to identify individuals who should be precluded from boarding flights, and the Selectee List Procedures security directive, directing domestic air carriers to conduct checks of passenger information against the Selectee List to identify individuals who should receive enhanced screening (e.g., additional physical screening or a hand-search of carry-on baggage) before proceeding through the security checkpoint. (GAO, 2008, September 9)

As of mid 2008, the TSA reported that 2500 unique individuals (250 Americans) were on the no fly list, while 16,000 were on the selectee list and 400,000 individuals were on the comprehensive terrorist watch list. These numbers represent a dramatic reduction from the previous year, when the no fly list had 44,000 names and the selectee list 78,000. The master, consolidated list is maintained in the Terrorist Screening Database at the TSC center. The TSC, created in December 2003 by Homeland Security Presidential Directive 6 (HSPD-6), was designed as a single point of contact to help screeners and police identify people with possible ties to terrorism. The DOJ IG report describes the information architecture of this “upstream” database:

The TSC shares the terrorist information contained in the TSDB by sending it “downstream” to other government screening systems where frontline screening agents can use the information to identify individuals against TSDB records. The following are examples of three databases that contain information from the TSC’s consolidated watchlist: (1) an employee of the U.S. Customs and Border Protection (CBP) agency at a U.S. port-of-entry searches the DHS’s Interagency Border Inspection System (IBIS) to determine if a person should be granted access to the United States, (2) a state police officer stops a vehicle for a traffic violation and queries the driver’s name in the FBI’s



National Crime Information Center (NCIC) system, and (3) a State Department consular affairs official searches the Consular Lookout and Support System to determine if a foreign national should be granted a visa to visit the United States. The TSC reported that approximately 270 million individuals are screened by frontline screening agents and law enforcement officers each month. (U.S. DOJ, 2007, September, p. v.)

It is difficult to say how many different lists are maintained all together, even with the TSA alone. A 2003 GAO report listed 12 different watch lists that were maintained by nine separate agencies prior to the opening of the DHS. Among these lists were the NoFly and Selectee lists maintained by the TSA, the “Warrant Information” list, containing all individuals with existing federal warrants, maintained by the U.S. Marshalls, the “National Automated Immigration Lookout,” containing the names of individual with expired, fraudulent or no immigration papers, maintained by the INS, and the FBI’s Violent Gang and Terrorist Organizations File (VGTOF). The report recommends the consolidation, centralization, and sharing of watch lists, but notes that software and hardware incompatibilities presented considerable obstacles to achieving this (U.S. GAO, 2003).

According to a report by a *USA Today* journalist, as of late summer, 2008, the TSA was maintaining a list of 16,500 people who had forgotten to bring their IDs to the airport and were subsequently forbidden from boarding. These names, according to the report, were listed in a larger TSA database that included names of people who had undergone greater scrutiny during the screening process or who were questioned by police for suspicious activity. Although the story does not mention the database, it appears likely that it is the Tactical Information Sharing System (TISS) operated by the Federal Air Marshal Service (FAMS). According to the February 2006 edition of *The Police Chief* magazine:

The Federal Air Marshal Service Tactical Information Sharing System enables federal air marshals and other law enforcement officers to create and instantly send reports of suspicious activity to the Federal Air Marshal Service Investigations Division for analysis and investigation. The resulting surveillance detection reports (SDRs) are shared in real

time with other federal, state, and local law enforcement and intelligence organizations (Quinn, 2006, n.p.).

Before the *USA Today* story was published, a TSA representative notified the reporter that the policy would change and that they would no longer store the name of individuals who did not bring ID. Other suspicious activity, including the attempted use of a fictitious name, would continue to be logged, however. Currently, the impact of appearing on these lists appears to be limited to air travel restrictions. It is easy to see, however, how a color-coded system of risk assessment could move from air-travel to all domestic travel and to the world of work. The template of “critical infrastructure” is already in place, providing a natural argument for the adoption of a similar system for employers in this domain. In fact, early discussions of the Real ID initiative suggested just such a system (McCullagh, 2008).

#### WATCH LISTS UNDER THE RULE OF LAW

Watch lists are particularly problematic for the interface between the state and its subjects because of the lack of accountability, due process and judicial oversight:

One agency, such as the FBI, “nominates” someone to be “placed on a watchlist.” That’s just a nomination, not a decision, and at most is directed toward putting a name on a list - a purely internal government function — not imposing any sanctions that would be subject to due process. Other departments of the or under the direction of the FBI, the National Counterterrorism Center and the Terrorist Screening Center, enter the nominated names into watchlists. They aren’t really responsible for any decision, of course, since they rely on the “derogatory” information provided by the nominating agency. Finally, the CBP, TSA, and other departments and agencies order airlines and other private companies, including common carriers, to deny services to people on those watchlists. But they aren’t making any decisions about who can fly, they say — they are merely enforcing a list that someone else has created.

The end result is that, as intended, it’s impossible to hold any specific agency or department responsible for the administrative decision to impose sanctions against a particular individual. And that, in turn, makes it impossible to obtain due process or judicial review. (“Time to Stop Tinkering,” 2009, n.p.)

What factors flow into the decision about whether or not a person will be targeted for increased, extended surveillance? This is a critical question, with different answers for each

country. In the U.S., it is part of conventional wisdom that most citizens are not the object of this extended monitoring. It is also part of conventional wisdom that policing agencies don't generally begin to focus their attention on you until you commit a crime. If a specific crime is committed, certain people may become suspects, or "persons of interest." Being present on a list does not necessarily mean you have committed a crime, however. Instead, you are a person of interest.

This term, "person of interest," turns out to be highly problematic, most importantly because it has no formal legal definition:

Officially, "person of interest" means...well, nothing. No one has ever formally defined it - not police, not prosecutors, not journalists. The terms "accused," "allege," "arrest" and "indict" all are dealt with in the Associated Press Stylebook, but there is no listing for "person of interest." Similarly, the U.S. Attorneys' Manual — the official guide to federal criminal prosecution — uses the terms "suspect," "subject," "target" and "material witness," but "person of interest" gets no mention. (Shaw, 2006, n.p.)

Despite (or perhaps because of) the ambiguity of the term, its use in government circles has grown. Linguist Roger Shuy provides a brief etymological history:

We don't know exactly when *person of interest* elbowed its way into use by law enforcement but it's likely to have shown up sometime in the 1970s, and then it really got noticed about the time of the 1996 Olympics bombing in Atlanta. You may recall that at that time the FBI leaked the name of Richard A. Jewell as a *person of interest*. Jewel was eventually exonerated, sued the media rather successfully for tainting his reputation, and got a public apology from the then Attorney General, Janet Reno. The phrase, *person of interest*, seems to be filling a lexical gap these days, undefined and vague though it may be, indicating a person who is somewhere between a suspect and a pure guess. You'd think law enforcement might have learned a lesson from the Jewell case (and a few others since that time), but not so. They've used it several times since... (Shuy, 2008,n.p.)

The term, as it is used today, is largely a justification for increased scrutiny and sometimes a formal announcement of suspicion. It is highly resonant with the Chinese "targeted person" (see chapter 6) though perhaps more difficult to quantify. Just how many U.S. residents are "persons of interest" at any one time? Clearly, any time an American appears on a "watch list" they become a person of interest. But what kind of behavior can get you on such a list? As

the number of official seekers of suspicious activity continues to multiply, the number of different actions that can get you on a list will expand as well.

The FBI admits that it is “common” for people to be placed on watch lists inadvertently. Chicago FBI spokesman Ross Rice has described one scenario in which a known terrorist dials your number by mistake. You pick up the phone and say hello, and the other side immediately hangs up. Although you have done nothing but pick up the phone, you have become associated, via the pen trace, with a known terrorist (Gallagher, 2007). Now you are a suspected terrorist and on a list, stored in multiple locations, including the consolidated TSDB at the Terrorist Screening Center, which as of late summer 2008 had 400,000 names.

The problem posed by government watch lists can be considered a subset of the more general problem discussed by Gandy (1995).

There is no question that from the perspective of the service provider, the use of an automated classification that supports the avoidance of risk is rational and profitable. From the perspective of the individual looking for a job, for housing, for insurance, or even for information to guide a purchase decision, the fact that they were denied service, or a discount, or were assigned to a queue, provides little information about the nature of or the basis for their classification. Indeed, the difficulty in knowing how these different pieces of information contribute to one’s classification represents a fundamental challenge to the pursuit of informed consent as a condition of fair information use. (Gandy, 1995, p. 44)

In both cases, state government and private companies, the data subject is entirely unaware of both the data used and the algorithm applied to make a particular risk assessment. In both cases there is a significant asymmetry between the information held by the risk assessing actor and that held by the subject, as well as numerous opportunities for the assessment process to be compromised by error. While in commercial circumstances such errors may result in a range of inconveniences, from not getting the best price at the grocery store to being denied a mortgage or job, errors in the state system could lead to an individual being wrongly incarcerated, beaten or killed.

Neither process, not the state assessment of terrorism/crime risk and not the business/profit risk, is transparent to the data subject. Neither process opens up satisfactory mechanisms of redress that exist for other forms of state record systems fitting with in a SORN/PIA framework. Both processes are fed by potentially unlimited, semantically broad sources of data which require techniques for parsing and merging into a single data system.

Both the state government and private sector entities have similar interests in aggregating data and running risk algorithms on that data, so tools developed in either class of institution may well apply to the other. There are no current legal boundaries to the sharing of these types of innovations, across the public -private boundary. One can expect continued discussion and coordination between the public and private sector in this regard, mixing in forums such as the second Government ID Technology Summit in 2007 in Washington, D.C., cosponsored by Digimarc and Viisage and featuring presentations from a range of government officials.

## CONCLUSION

This has not, could not have been, a comprehensive description of the state dossier system (SDS) in the U.S.. I have shown that the number of SoRs that flow into the U.S. SDS is high and that the names of key systems changes regularly. By approaching this topic from a general semantic frame rather than initially targeting one or two institutions or SoRs, the process of analysis has been more open to identifying more general, transferable and transposable components that are likely to underlie any modern state dossier system. While it is natural to question whether or not the state has that all-comprehensive database with personal data on

everyone (a mother of all databases MOAD), such a potential reality lies outside the purview of public records discovery.<sup>32</sup>

Although we have trouble describing with any confidence the potential configuration of the U.S. MOAD, we can see evidence of increasingly centralized data warehouses with large stores of personal information of both criminals and non-criminals. This information can persist for decades and is available to afford a decision, by algorithm or by person, at any future moment as long as this data persists. Today, we know that data within the IDW is likely fed into algorithms at the TSC, with some of it tripping watch list nominations for the data subjects.

We must not underestimate the value of “notice” as a Fair Information Principle and how its encoding into both the Privacy Act of 1974 and the E-Government Act of 2002 has made the present investigation possible. While there is likely to be much we are not aware of, the information that has been released to the public to date under the rule of the Privacy Act is of high volume and detailed. While other principles are often ignored or put aside on the basis of various intelligence and law enforcement justifications, notice remains viable enough that it helps to paint a vivid picture of the many ways the U.S. government has changed its orientation to the production and collection of personal information.

If we think of the U.S. SDS in terms of specific projects like TIA, TIPS, CAPSS II, or Real ID, it is possible to make the argument that the American system of government has worked, that public opinion has helped to stop and defund executive branch plans to extend record keeping and data sharing for the “innocent until proven guilty” citizens. But if, instead, we look at the generic dossier tools and system components that underlie these programs, government gets what it wants. In fact, one could even say there is an air of authoritarianism in the way that the

---

<sup>32</sup> For an extensive discussion of the search for the U.S. MOAD during the original data gathering process, please see *Appendix A*.

U.S. executive branch, along with the DHS and intelligence agencies, have continued to advance particular components and record systems against clearly stated public will, including the law. Real ID may be dead but the Enhanced Driver's License, complete with proximity RFID is alive and well, available or (as of summer, 2009) immanently available in seven states with a combined population of more than 90 million. TIPS was excoriated by the public and outlawed by Congress, but a nationwide suspicious activity reporting system is now a major and growing program complete with its own XML standard. Watch lists and risk color-codes have been flatly rejected by the public and Congress, at least until clear channels for redress are offered, but the ATS and Secure Flight programs, indexed to the consolidated watch lists of the TSA, move forward anyway. While the ATS program today is limited to those traveling internationally, the amount of data that is collected on regular American travelers greatly exceeds the boundaries of any reasonable security program.

We can see that the federal government wishes to avoid certain information architectures, but only in certain contexts, so that they can more easily claim that the initiatives underway are not part of a national ID or state dossier system. Having a central, federal database linked directly to a nationwide ID system appears to be too close to a general model of a dossier system for the government to push for. Instead, the new system for verifying identity is likely to be based on a federated architecture in which an interface has the power to query and display data but the data remains stored, and under the control of, the local system. We see this same pattern as part of the new ISE shared spaces concept for the circulation of suspicious activity reports. One can argue just how significantly different the federated architecture would be in practice from a more physically centralized model, but it would miss the fact that the other systems, like the IDW, do store data on their own and can benefit significantly from a nationwide ID system without being formally linked to it.

Suspicious Activity Reports represent a major change in balance between criminal investigations and domestic intelligence, not only returning to an era in which human rights abuses are well documented, in which the “dossier” is used as an instrument of political power, but exceeding anything known in the past century. Although the TIPS program was firmly rejected by the public and outlawed by Congress, the current configuration of SAR reporting nationwide is in many ways more sophisticated than the original plan. Rather than anchoring the reporting system on a large network of professional of all stripes, the nation’s 800,000 local police are beginning to receive training as intelligence agents. Further, under the auspices of fusion centers, an as of yet undetermined number of utility workers, fireman and regular police are being enrolled as Terrorism Liaison Officers. Given we already have evidence that military agents and police have produced and stored files on peace activists and tax protestors within the past decade, there is clearly reason to be concerned.

Watch lists, reasonable in moderation (the “10 Most Wanted”), are distinctly undemocratic in character as they grow in use. Since ones presence on a list does not necessarily indicate conviction or indictment for a crime, it is not subject to judicial review. Presence on a watch list can mean the individual will be mildly inconvenienced, deprived of their First Amendment rights to assemble and associate, denied credit or a job, or even be subject to physical abuse and harm, all without clear rights to challenge.

The interaction between watch list and SARs is potentially very dangerous, as it combines two activities that are largely exempted from judicial review. As the government argues, with sound logic, that publishing its algorithms for identifying suspected terrorists to the public, or making its comprehensive list of names publicly available, would dramatically compromise their ability to identify and apprehend individuals preparing to do this nation harm. While this logic is defensible, it becomes indefensible when the practice of producing watch lists



grows to include not just shady international travelers with checkered pasts but the entire mass of the traveling public. It is clear that SARs do flow into databases like the IDW and from there to the TSDB. Individuals who have been flagged with multiple SARs (which by definition means there is suspected association with terrorism) are likely to appear on a watch list and bear the consequences on their life chances. If the list turns out to be one that is circulated in the private sector, as are the TSA's no-fly and selectee lists, the chance for harm grows.

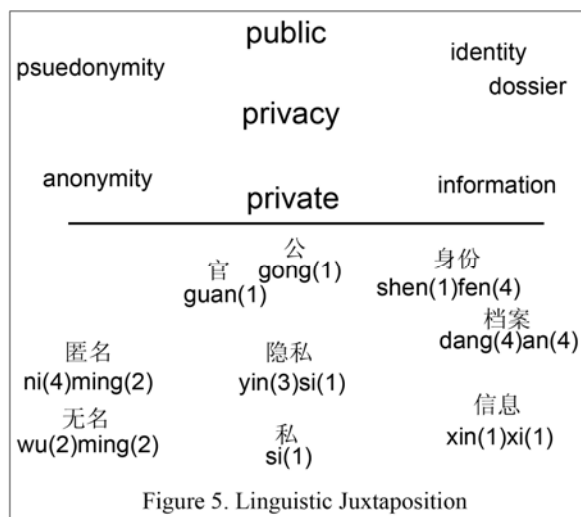
In the next chapter, "Privacy Across Cultures," I set the stage for introducing China as a point of comparison, for the purposes of both honing the language of state dossier system problematization and better gauging the severity of the U.S. case today.

## CHAPTER 5: PRIVACY ACROSS CULTURES

This chapter has two primary goals: 1) to establish common ground for the problematization of state dossier systems connecting two highly distinct case studies on the basis of information privacy and 2) to advance the academic discourse concerning the role and meaning of privacy within the global context of surveillance studies. In the interest of regaining some core clarity and analytical utility for the word, this chapter explores the dynamic interrelationship between American and Chinese cultural and legal approaches to the negotiation of “privacy.” “Privacy,” as used here (with quotes), is meant to be a protean term that stands in for the highly complex semantic/discursive networks that surround inter-cultural dialog centered on this English word.

In this chapter I explore this linguistic relation via four points of juxtaposition: privacy translated into Chinese as “*yinsi*,” the notion of “reasonable expectation” of privacy, the public-private dialectic, and finally the notion of anonymity. These nodes are not entirely distinct from each other and have important interactions.

The diagram to the right is intended to provide a quick, visual orientation to a linguistic juxtaposition of English and Chinese privacy. These are words that come to mind, that tend to become part of conversations in which privacy is discussed and negotiated. Words from each rectangle that have similar row-column cell positions



reflect their equivalence in typical dictionary translations. For, example, privacy and *yinsi* both

occupy the center positions of their respective rectangles; *gong* and public both occupy the middle of a top row. Within a rectangle, words along the central vertical axis are considered to be more closely related than those with significant horizontal separation. Maximum vertical separation suggests that the terms commonly appear in opposition.

It is important to note that this map is for heuristic purposes and is not intended to represent some definitive “semantic field” surrounding the word privacy. I argue only that, based on my comprehensive review of literature falling within the general state dossier system rubric, these words appear to play an important role in the privacy discourse of both countries. Given today’s U.S. political climate, the word “security” is quite frequently seen and heard in discourse on privacy, but perhaps not nearly as frequently in China. Other words, like “secrecy” or “trust” could also have appeared, but they are not the subject of the present exploration. This is a selective representation. It is intended to help orient the reader to the exposition that follows, and to illustrate how such maps can help us to better understand the social dynamics of meaning.

The first juxtaposition, the linguistic equation of privacy with *yinsi*, is a critical space to start. Translation is a highly complex process rife with unfounded assumptions and embroiled in power politics (Liu, 1995). Social systems constitute themselves in language, thus making words the basis of the reality we experience (Austin, 1962; Berger & Luckmann, 1966; Rorty, 1989; Searle, 1995). The remaining three nodes reflect areas that have their own powerful tensions and ambiguities within Western discourse that cry out for a more informed universal pluralism. The notion of “reasonable expectation” of privacy is a key term in the legal justification of privacy interests in the U.S. and has a common sense interpretation that translates easily across modern languages. The notion of public and private space has been debated for at least as long in China as it has in the West, where scholars seem increasingly dismayed at the possibilities for conceptual coherence. Finally, anonymity in both language and practice has a complex

relationship to the public-private dynamic and to the privacy concept itself that is not always clear.

### PRIVACY = *YINSI* ?

It is surely telling that the characters that make up *yinsi*, the Chinese word for “privacy”, carry the connotations of illicit secrets and selfish, conspiratorial behavior. (“The long march to privacy,” 2006, p. 45)

. . . analytical categories cannot operate fruitfully in a transhistorical, transdiscursive mode. But neither do I think that cultural relativism provides a viable solution in this fast shrinking world of ours, in which geopolitical boundaries are constantly being redrawn and crossed, and in which the need for translation and interaction is literally thrust on people who had little contact before. It seems to me, that to eschew transhistorical/transdiscursive approach on the one hand and cultural relativism on the other, one must turn to the occurrences of historical contact, interaction, translation, and the travel of words and ideas between languages. (Liu, 1995, p. 19)



It is certainly true that in terms of the broadest possible mapping of Chinese and Western inter-discursive structure, we can say that the translation for privacy is *yinsi*. This is the translation you will find in any major Chinese-English dictionary. Young Chinese use the term to refer explicitly to what most Western academics would agree are a kind of privacy rights, and it is the word one sees used in the growing number of privacy-related court cases and mass media stories, but there is much more to the Chinese concept of privacy, as I explain in detail below.

### COMPOUND WORDS AND NEOLOGISMS IN CHINESE HISTORY

There is an important distinction within the Chinese language between individual character words and compound words. It is generally accepted that early forms of the Chinese language (up to the Qin dynasty, 221 BC- 206 BC) consisted primarily of monosyllabic words represented by individual Chinese characters (Tai & Chan, 1999). Compound words began to appear during the Han dynasty (206 BC-220 AD) but have increased substantially in modern

times, from roughly 20% percent of the written lexicon before the Qin dynasty to more than 80% today (Shi, 2002). The pre-modern Chinese written language, today known as classical Chinese, retained a strong monosyllabic character throughout its use well into the 19<sup>th</sup> century. Only a tiny percentage of the population, scholars and government officials, could understand classical Chinese, or manage the often ambiguous, highly contextual meanings which clustered around each individual character (Rosemont, 1974). Spoken language tended more toward compound words in which the meaning of single characters were joined or blended to produce different, usually more specific connotations. The Chinese *baihua* movement led by literary celebrity Lu Xun, began to adopt more common language in written form, making it at once more colloquial and understandable to the average Chinese. With its marked increase in the size of its vocabulary, *baihua* was more able to mediate the rapid pace of intellectual and cultural development that was occurring at the time. Early 20<sup>th</sup> century Chinese thinkers began to incorporate a large number of compound neologisms, many imported from the Japanese, to translate Western concepts, such as the use of the compound *quanli* for “rights.” It appears that the word *yinsi* is a recent neologism whose use has been heavily influenced by exposure to both Western legal scholarship and popular culture in the mid- to late- ‘80s (Zhu, 1997; McDougall, 2004). As is discussed in detail below, “privacy rights” (*yinsiquan*) have growing cultural salience and legal force today.

It would be a mistake, however, to make the apparently logical inference that the Chinese simply imported the concept of “privacy” whole cloth. As with many other neologisms in Chinese discourse, they represent more recombinations and extensions of existing concepts and “are in many cases limited to catalyzing change or encouraging trends already underway” (Angle, 1998, pp. 623-624).

The transcription of the Chinese word for privacy into its official phonetic transliteration, pinyin, has been a cause of some misunderstanding. Although pinyin is a perfectly adequate

alphabet to reflect Mandarin phonetics, Chinese is a tonal language. Western journals and publications have often used pinyin transliterations without any additional tonal information. This can lead to confusion when two compound words with the same sounds but different tonal patterns are close in meaning, as is the case with *yinsi*. The proper pinyin transliteration for *yinsi* (privacy) is more accurately written as *yin3si1*, reflecting the fact that the first word of the compound is pronounced using the third, dipping tone, and the second word is pronounced with the first, steady tone. *Yin1si1* (two steady tones), on the other hand, means “shameful secret.” For simplicity, I will refer to *yin3si1* in this paper as *yinsi* and will not refer to this other, often conflated word again.

*Yinsi* (隱私) is a compound word, consisting of two characters that have independent meanings. Yin (隱), by itself, may mean secret, hidden or concealed. Si (私), by itself, can mean personal, private or selfish.<sup>33</sup> To understand more about the longer, more traditional Chinese concepts that inform the modern term *yinsi*, we must look more into the second word in this compound, *si*, and its meaning in Chinese political and social thought over the last several centuries. We will address this in detail, below, as part of a discussion on the public-private divide.

The equation of privacy and *yinsi* reflects a particular social, political, cultural moment in the interaction between China and the U.S. that is inseparable from relations of power and the contingencies of history (Liu, 1995; Venuti, 1998). To say that the Chinese have no equivalent concept for privacy is first to assume that there is a clear concept of privacy in the West. This, of course, is a highly problematic assumption, as was discussed in chapter one. As a reminder, for the purposes of this dissertation, I focus on “information privacy” and the two concepts of “boundary resources” and “contextual integrity.”

---

<sup>33</sup> See English-Chinese dictionary available at <http://www.mandarintools.com/worddict.html>

In America, the meaning of “privacy” and its relative importance compared to other values such as security and accountability has fluctuated over time. Best et al. (2006) identify three major developments that may have had an effect on contemporary public sentiment toward privacy: 1) the emergence of the Internet; 2) the commencement of the war on terror; and 3) the development of a wide array of new surveillance technologies.

Clearly, the salience of September 11<sup>th</sup> is much greater for Americans than it is for the Chinese, but the populations are both simultaneously experiencing the rise of networked electronic communication and technologies of surveillance. The lives of both Chinese and Americans are becoming increasingly intertwined on an Internet populated by global institutions like Google and Yahoo. The current moment almost demands a cross-cultural understanding of privacy, even if concise definitions are elusive and ultimately impossible.

In the U.S., there remains a great deal of confusion over how “privacy” can be effectively invoked within legal and technological contexts. Struggles over what a “reasonable expectation” of privacy is, the public-private divide and the meaning and practical utility of “anonymity” represent three areas of particular discursive tension. Below, I examine each of these areas in turn.

## REASONABLE EXPECTATION OF PRIVACY

All visitors should be aware that they have no reasonable expectation of privacy in public or private locations (U.S. State Department Travel Advisory on China, March 2008).

If “reasonable expectation” is interpreted in a strictly legal sense, the U.S. State department might be considered correct in its above assertion. As was noted in chapter 3, however, the notion of “reasonable expectation” in legal discourse has weakened constitutional protection of the privacy of American citizens over the past several decades. The problem with reasonable expectation in the U.S. has been that what is reasonable changes with the winds of

culture and politics and allows for no definitive boundaries. Clearly our “reasonable expectation” of privacy today is much less than it was in 2000. Even before 2000, changes in the way public space was subject to routine surveillance might have been, but were not, curtailed by a strong expectation of privacy in public. Today, there are no significant laws protecting American citizens from routine surveillance in public by either public or private entities. As we will see in China, the public appears to have a stronger privacy consciousness within this context, a fact which is also reflected in major municipal laws which restrict the deployment and use of such systems.

The reasonable expectation of privacy for Americans online is in considerable flux today. In the summer of 2007, the U.S. Ninth Circuit Court of Appeals ruled that Americans do not have a reasonable expectation of privacy in the IP addresses of Web sites they visit (Singel, 2007a). Although there has been some confusion on the matter, the July 2007 of the U.S. Sixth Circuit Court of Appeals ruling in the case *Warshak vs U.S.* held that Internet users do have a reasonable expectation of privacy in the content of their e-mail, whether it is stored on their home computer or at a third party ISP. The U.S. Justice Department indicated it planned to appeal the decision.

#### REASONABLE EXPECTATION OF PRIVACY IN CHINA

Even though China (like the U.S.) does not have explicit constitutional protection for “privacy,” its statutory system comprises a growing array of legal protections, anchored by the declaration of an explicit “right to privacy” in the 2002 draft of the Chinese Civil Code.<sup>34</sup>

---

<sup>34</sup> Some examples, excerpted from Privacy and Human Rights 2003, published by Privacy International and retrieved July 1, 2008 at <http://www.privacyinternational.org/survey/phr2003/countries/china.htm>:

The Law on the Protection of Minors (1991) provides that "no organization or individual may disclose the personal secrets of minors" and "with regard to cases involving crimes committed by minors, the names, home addresses and photos of such minors as well as other information which can be used to deduce who they are, may not be disclosed, before the judgment, in news reports, films, television programs and in any other openly circulated publications. [904] The Law on the Protection of Rights and Interests of Women (1992) provides that "women's right of reputation and personal dignity shall be protected by law. Damage to women's right of reputation and personal dignity by such means as insult, libel or giving publicity to private affairs shall be prohibited." [905] The Law on Lawyers



Statutory protection was judged strong enough by analysts for *Privacy International's* "2007 International Privacy Ranking" to rank higher than that of the American legal system. Although this appears on its face to be an absurd assertion, the claim holds up under initial scrutiny (at least if we focus solely on the letter of law).

The formal definition for "right to privacy" introduced into the 2002 draft civil code (similar to Restatements in U.S. law) defines the right to privacy in the following way:

- 1) the subject of the right to privacy can only be a natural person;
- 2) the objects of the right are private activities and personal information;
- 3) the scope of the protection of the right is limited by public interest

(Cao, 2005, p. 651).

It should be noted, firsthand, that the promulgation of this new specific right to privacy is not simply a product of changing domestic public sentiments and their effect on policy makers, but likely results from a range of both domestic and international pressures. According to McDougall (2004), the context of the law's passage "suggests that the code was developed as part of an international legal framework dominated by the free market ideologies of the World Trade Organization and the government of the United States" (p. 6).

Note, also, that the third line of the definition maintains the supremacy of the "public interest" over privacy in Chinese law. Although it would be easy to suggest that the public interest clause essentially renders impotent the right as otherwise defined, issues of "security" clearly play a similar role in the U.S.. Further, public concern over private, corporate abuses of personal information appears to have drawn a sympathetic ear from the Chinese government. There is growing talk of a new national law to regulate such practices. Before rejecting Privacy

---

(1996) requires lawyers to protect the personal secrets of their clients; [906] the Law on Statistics (1983) provides that data collected from investigations shall not be disclosed without the consent of data subjects; [907] and, the Provisional Regulations Relating to Bank Management (1986) provide that all information.

International's findings too quickly, it's worth reminding ourselves that U.S. policy makers are unlikely to support generalized privacy laws that would be deemed too restrictive of business practices. As we will see below, it is clear from recent citizen actions in public and via China's courts that the "right of privacy" is gaining real force.

#### GAUGING PUBLIC SENTIMENT

Another key aspect of the legal notion of reasonable expectation is the relative salience and strength of privacy within the public at large. The public expectations of privacy in America today are also in flux. It is commonly stated in contemporary discourse that Americans value privacy less than they did before September 11<sup>th</sup>, that privacy has become an antiquated value in a world where instability seems to lurk around every corner. Although there is certainly some truth to this assumption, the available data shows a much more complex picture. While it is clear that privacy took a back seat for many Americans during the immediate aftermath of the attacks, most polls have shown that concern for personal privacy from government institutions has mostly been on the upswing since sometime in 2002 (Best et al., 2006). Still, a 2008 national poll conducted by Rasmussen Reports shows that Americans, by a narrow margin (51% to 49%), value their security more highly than they do their privacy ("51% Say Security," 2008).

Another common assumption is that America's Facebook and MySpace-happy youth do not value their privacy in quite the same way that their parents did. There is certainly an element of truth to this. A Zogby poll conducted in early 2007 found that only 35.6% of 18 to 24-year-olds considered the posting of their picture in a swimsuit online to be an invasion of privacy, compared to 65.5% for those 25 and older ("Poll Exposes," 2007). Younger Americans are more concerned, however, about their privacy in relation to government institutions than older citizens (Berton, 2006).

Public opinion polling on privacy related topics is limited in China compared to the U.S., but has recently been on the upswing. As we will see, we can also get a reading of public sentiment from activity in the courts and direct demonstrations of public will.

A survey conducted in 1997 of residents of five major Chinese cities showed strong privacy awareness for personal feelings, marital relations, diaries and other personal documents, with 73.6% agreeing to the statement, “Do not read a colleague’s files and documents without his or her permission,” and 71% agreeing to the statement, “Parents should not read their child’s diary.” Survey results indicated that privacy was more valued among better educated, higher-paid, younger, and female respondents (McDougall, 2002, p. 167).

Chinese citizens share an aversion to spam with their American counterparts. China, once the source of much of the world’s spam, has dramatically reduced this problem with concerted government and industry intervention. A law regulating the sending of spam drafted by the Internet Society of China (ISC) went into effect in March of 2006 (Wu, 2006). Spam was the subject of a recent major Chinese Central television investigation, timed to be shown on World Consumer Rights Day, March 15. In March 2008, China’s largest cellular telephone operator, China Mobile, was forced to publicly apologize after Internal security lapses allowed seven advertising firms to send more than 200 million spam messages via China Mobile and the second largest provider, China Unicom. The first civil suit in China over SMS was recently filed in the Beijing Xicheng District Court (Jiang, 2008). Much of the talk of a general privacy law, promised for 2008 but which appears to be delayed at least a year, has to do with the unrestricted exchange of the personal information for which spam is but one problematic manifestation.

Surveys conducted over the past few years by a leading national newspaper the China Youth Daily (CYD) show significant and growing interest in the personal privacy. A survey

conducted in May of 2006 found that 91.8% were “worried that their private information can be too easily divulged and misused,” while 74% called for tougher laws to protect privacy. A survey in January 2007 showed that the China’s online population overwhelmingly (83.5%) disapproved of a plan to require real name registration for all bloggers and BBS users.

Increasingly, emerging public sentiments about privacy are bubbling up into the court system. Below are a few examples.

In early 2004, two recent graduates of Shanghai’s Fuxing High School, male student Wei Gang and his (unnamed) girlfriend, sued their alma mater for invasion of privacy. The school, which had set up CCTV cameras in the classrooms, filmed and rebroadcast, school-wide, a passionate kiss between the two young students. Wei and his girlfriend asked the high school to publicly apologize, both in the China Youth Daily and on school campus. In addition, they demanded 10,000 Yuan (USD\$1,205) for mental anguish, claiming they had been ridiculed at school so much that their performance on college entrance examinations suffered and the girlfriend even contemplated suicide. The Shanghai Hongkou District People’s Court decided in favor of the school, agreeing that it had the right to monitor its students and that their presence in a public space negated any privacy claims (“Court Rejects,” 2004). Though they lost their court action, the students gained considerable public sympathy (York, 2005).

In early 2007, Guo Li, a lawyer from Hangzhou, sued Internet search engine Baidu.com for publicly exposing a copy of his e-mail online. The case was heard in Hangzhou Xiaoshan District People’s Court in December 2007. Guo was suing Baidu and Hi China for 1,000,000 RMB because of its claimed failure to adequately respond to requests that the exposed e-mails be deleted (“Baidu Accused,” 2007). In the spring of 2008, the Hangzhou Court decided in favor of

the defendants, arguing that not enough evidence had been provided to suggest that they did not respond to Guo's requests in a timely manner (Qu, 2008).

In the fall of 2007, Beijing University student Lu Feng decided to take Microsoft to court over its decision to implement Windows Genuine Advantage in copies of Windows XP distributed in China. Lu argued that WGA tool is akin to spyware, and that both his "right to privacy" and the property right in his PC were being violated. Lu's suit echoed a similar claim ongoing in the United States District Court of Seattle, *Brian Johnson vs. Microsoft*. The First Intermediate People's Court of Beijing accepted this case for review, though this is not to be taken as a judgment of its technical merits (Fisher, 2007).

Early in 2008, a young couple in Shanghai decided to sue a metro station after a video of the two kissing in the station was posted online at video sites including YouTube. The couple claimed that their privacy rights had been violated, an argument that was supported by Chinese legal scholars quoted in mass media. Employees of the metro company involved in the video distribution were fired from their jobs and the company has been negotiating with the couple over financial compensation ("Kissing Couple," 2008; "Shanghai Subway," 2008).

Do the Chinese have a "reasonable expectation" of privacy as they go about their daily lives? Is this expectation protected by law? Although the context may vary, Chinese expectations appear comparable to other modern societies. To understand how the expectation of privacy in China relates to that in the U.S., we focus now on the notion of public-private divide.

## PUBLIC-PRIVATE DIALECTIC

The public-private dialectic has been applied in radically different ways in Western discourse, with each pole mapped to different theoretical entities within the social system. Habermas's (1989) theory of civil society, for example, views the public sphere as a domain separate from that of the state. The public-private dichotomy may also reflect a contrast between government-owned institutions and private institutions such as corporations (Weintraub & Kumar, 1997).

Despite these differences in application, it has been generally believed that the boundaries were easily discernible, often physically tangible, and could "demarcate a dichotomy of realms" (Nissenbaum, 1998). The walls of a house or an apartment, for example, physically traced a boundary between the private space of the home and the outside world. An open park was a public space, bounded by surrounding streets. The skin and clothes of an individual traced a clear boundary between an individual and the outside world. The categories of territorial privacy and bodily privacy mapped well onto the public-private divide and, especially within American society, appeared to reinforce each other.

Although much discourse on privacy in the West deals with the notion of a public-private dialectic, it has been marked by frustration over the increasing fuzziness of the concepts in the world of electronic networked communication and high tech surveillance (Marx, 2001). Passerin d'Entreves & Vogel (2000) note that the two concepts comprise "a family of distinctions that are constantly shifting under the twin pressures of social change and political contestation" (p. 1). Electronic, networked media, with their nodes increasingly saturating global space, are



constrained more by logical and less by physical boundaries. This loss of the role of physical boundaries in affording boundary negotiation renders a number of well rehearsed strategies for privacy maintenance obsolete.

With information technology, our ability to rely on these same physical, psychological and social mechanisms for regulating privacy is changed and often reduced. In virtual settings created by information technologies, audiences are no longer circumscribed by physical space; they can be large, unknown and distant. Additionally, the recordability and subsequent persistence of information, especially that which was once ephemeral, means that audiences can exist not only in the present, but in the future as well. (Palen & Dourish, 2003, p. 2)

There has been a dramatic reduction in the distribution of social resources for personal boundary negotiation as a result of these changes to the primary media of communication. As human interaction continues to shift to electronic networks, traditional schema for boundary negotiation often lose their utility (Meyrowitz, 1985; Shapiro, 1998; Nissenbaum, 1998, 2004).

#### PUBLIC AND PRIVATE IN CHINESE DISCOURSE (*GONG-SI*)

In Chinese discourse, the binary relation *gong-si* (公 - 私) roughly mirrors the Western binary notion of public-private, occupies more than 2,000 years of history, and has its own attendant ambiguities (Rowe, 1990). Evidence that the two words, *gong* and *si*, emerged largely as paired opposites can be found in the third century BC Chinese dictionary *Er ya*, which defines *gong* as simply “not *si*” (*wusi*), while the first century *shuowen* defines *gong* as “turning ones back on the private” (Rowe, 1990, p. 316).

*Gong*, by itself, can mean “just,” “honorable,” “public,” or “common.” Some important compound words in which *gong* appears include *gongan* (公安), public security; *gongdao* (公道), justice; *gongguan* (公關), public relations; and *gongmin* (公民), citizen. *Si*, by itself, can mean personal, private or selfish. Compound words that *si* appears in include *siren* (私人), individual/private; *siyou* (私有), privately owned; and *sili* (私利), personal gain.

Although much of China's neo-Confucian scholarship has considered *si* to be synonymous with selfish interests, there have been important exceptions, especially during the late Ming and Qing dynasties (Angle, 2002). Perhaps most notably, the writings of leading scholar/journalist of the late 19<sup>th</sup> and early 20<sup>th</sup> century, Liang Qichao, argued that the public welfare *gong de* (公德) was dependent upon a bounded private domain *si de* (私德) where thought could be cultivated.

Just how the *gong-si* dialectic is applied to real-world events and issues is as varied in Chinese culture as it is in the West. It is generally agreed in academic circles that attention to and salience of *gong* has been far greater than *si* for much of the country's history (Wakeman, 1998; Angle, 1998; McDougal, 2002). In the past, *si* might have been used to apply to an emperor, the official head of state, where the relationship between *gong* and *si* was between the selfish interests of the ruler and the true interests of his collective subjects (Zarrow, 2002). Another way of mapping *si* is to the family or even an individual scholar's walled study (Furth, 2002), against the open sphere of the collective *gong* public.

*Gong* and *si* are protean terms. In traditional and early modern Chinese thought, *si* could represent both individual and collective interests (usually the family, but also clans) when considered in opposition to state interests. Madsen (2007), quoting eminent Chinese sociologist Fei Xiaotong, reminds us that the distinction between public and private in Confucian thought is "completely relative":

Sacrificing one's family for oneself, sacrificing one's clan for one's family - this formula is an actual fact. Under such a formula what would someone say if you called him *si* [acting in his private interest]? He would not be able to see it that way, because when he sacrificed his clan, he might have done it for his family, and the way he looks at it, his family is *gong* [the public interest]. When he sacrificed the nation for the benefit of his small group in the struggle for power, he was also doing it for the public interest [*gong*], the public interest of his small group. . . . *Gong* and *si* are relative terms; anything within the circle in which one is standing can be called *gong* (p. 5).



Scholars in general appeared to value their solitude as a place for reflection and creativity. Focusing on the words of a 17<sup>th</sup> century poet, Furth (2002) shows how private, secluded spaces were valued by the intellectual elite.

. . . the solitary recluse, as Cao Heng's poem says, can be indifferent to the gaze of others; in the eyes of the world he can appear shameless. He is freed to look at himself, turning inward to an interior landscape that, turning the world inside out, reveals a universe of his own creation (p. 53).

GONG, SI, GUAN

This protean nature of Chinese single character words gives them an inherent semantic flexibility across time, space and context that appears to exceed that of the public-private dialectic. An important strand of Chinese discourse includes *gong* and *si* as part of a tripartite distinction with *guan* (官), the official or state sphere (Rankin, 1993; Wakeman, 1998). In this model, *gong* exists at a medium point between *si* of the private home and individual and *guan* as the agent of the institutional state. Strand (1989) offers a compelling portrait of what this tripartite distinction meant during the early 20<sup>th</sup> century:

In China, the dependence of gentry and merchant opinion on official power (*guan*) was loosened during the late Qing and then broken under the Republic. Urban elites never gathered the strength and the will to support a fully autonomous public sphere. But the trembling of the state in the 1920s, the weak legitimacy of private interests (*si*), and the positive moral and political evaluation of *gong* as a zone of discussion and concern encouraged newspaper editors, new and old civic leaders, and ordinary citizens to improvise tactics and strategies for expressing political views in public. Thus constituted, city politics took on a life and a logic of its own as opportunities to engage in political discussion and action expanded. (p. 168)

Rowe (1990) has argued that the *gong/guan* distinction has persisted into modern times, and that “[d]espite the incontestable growth of central state power which culminated in the party state of the People’s Republic,” widespread continuing cultural and formal legal salience of this tripartite approach “seem to suggest a survival of an articulated intermediary ground between state and society more pronounced than that in the contemporary West” (p. 326). Rowe argues

further that the Chinese *gong-si* dialectic is more abstract and less implicated with spatial entailments than is the public-private divide of Western discourse, epitomized, perhaps, by the close association between public deliberation and open public squares.

*Gong*, then, can be understood as the truly collective interest that may or may not be in sync with official state interests. *Gong*, seen in this light, is none other than *si* in the aggregate, a philosophical approach with roots in early Confucian thought. Mencius, for example, describes the interdependence of private desires with the collective good.

According to Zarrow (2002), “*si*, though highly suspect, was to be understood as valuable in particular contexts” (p. 122). Although not necessarily a mainstream view within Chinese historical discourse, one could make an argument (citing notable scholars in a chain back to Confucius and Mencius) for *si*, not simply as an instrumental value, but an intrinsic part of a healthy, viable social system.

#### THE RISE AND FALL OF *SI*

In Chinese studies there is a common term, *fang-shou*, which refers to cycles of tightening and loosening of discursive rights and freedoms. One might think of the relative salience of *si* and its relation to *gong* as rising and falling across time in a similar fashion (perhaps parallel to) *fang-shou*. Although it is relatively easy to develop such a graph for the salience of *si* on its own, its relation with *gong* over the same period is more complicated — in part because of the addition of *guan* in this tripartite distinction, but also because of the way the uses and “meaning” of *gong* have changed over the long stretch of Chinese history. One could plot a relationship between *gong* and *guan* over time as well that would help to contrast periods where people felt the government to be acting in their interests (the communist revolution and its immediate aftermath) to those when corrupt officials actively disdained the true needs of their

people, but again always keeping in mind that the meaning of each of these words, especially *gong*, has had significant temporal and demographic variance.

As McDougall (2002) reminds us, “the meanings and values associated with *si* have not been uniform in Chinese history” (p. 10). Zarrow (2002) has argued that *si* rose to prominence in late Imperial China through the early Republican period, but began to reverse shortly after the 1949 communist revolution, reaching a nadir during the Cultural Revolution and the ensuing decade. Public expectations of “privacy” were likely at a low point in China during the years of the Cultural Revolution and its aftermath in the 1970s. In urban areas, residential space was so scarce that parents, children and relatives would often sleep in the same room. At the same time, communist ideology labeled any discussion of individual interests as “spiritual pollution”: the collective, *gong*, was the only reality. The complete lives (psychological, medical, intellectual, social, sexual) of virtually all citizens were kept in duplicate dossiers (*dangan*), one with the local public security bureau and the other with the persons “work unit” (*danwei*) and were updated and consulted regularly by agents of the state when making decisions (Lu & Perry, 1997).

When Deng Xiaoping’s modern economic reforms began to gather momentum in the mid ‘80s, public expectations of privacy began to grow with them, both at home and out in public. Ideologically, private interests were no longer vilified. Deng’s oft quoted comment, “it does not matter whether a cat is black or white, as long as it catches mice,” gave new legitimacy to private venture and the pursuit of individual profit, because it would mean greater wealth for the country at large. With modernization came steady growth in the size of available residential space (Lu, 2005):

This expansion of physical personal living space has created the objective condition for the protection of personal privacy. According to the Blue Book of Real Estate, from 1978 to 2003, per capita housing space in Chinese cities and towns has grown from 3.6 square meters to 11.4 square meters. Compared with Western countries, per capita housing space

in China is still not extensive, but it has made a great improvement over the conditions of 20 years ago. Society leaves a bigger physical space for the personal, which naturally makes it possible to extend the scope of what is included under the concept of “privacy” - even if this does not necessarily result in strengthening of idea of privacy (Lu, 2005, pp. 8-9).

Children (also in decreasing family sizes due to the one child policy) began to get their own rooms and soon were scolding parents for entering them without knocking, or sneaking a look at their diary, in replays of common scenes in the U.S. and other Western countries. Modernization freed the average Chinese worker from cradle to grave dependence on their work unit. With worker mobility came the decreasing significance of the *dangan*; employers tended to know much less about their employees than before (Lu & Perry, 1997).

In this society, people no longer regard individual interests, individual freedom, and individual rights as taboo topics of discussion. In contrast with the not-so-distant past, individual independence and subjectivity have obviously been promoted in their importance and value in social life. Increasing diversity in contemporary Chinese society also makes for greater variety in Chinese ideas of privacy. More and more Chinese citizens begin to give importance to privacy and express concern over protecting emerging rights to privacy. (Lu, 2005, pp. 7-8)

Increasing salience of *si* can be understood of an expansion of those conditions and situations that modern urban Chinese would include under the rubric of “reasonable expectation of privacy.”

#### CHINESE “PRIVACY IN PUBLIC”

Chinese valuation of territorial privacy and its conceptualization of the public-private dialectic appear to be complex enough to include some notion of “privacy in public.” Political advisors to Beijing’s municipal government are quoted in the Jan. 30, 2007 *People’s Daily*, voicing concerns over the use of surveillance cameras in public areas. The article points to the ease with which digital images can be manipulated and cites privacy concerns. Beijing established a city wide regulation on the use of cameras that went into effect on April 1. The regulation requires secure storage for pictures and videos captured by the cameras, and dictates

that they be installed only in conspicuous public places. A similar law was recently passed in the city of Chongqing.

There are no comparable laws in U.S. metro areas such as New York and Chicago where there has been a similar expansion of camera surveillance in public places. It would appear that as of today, the notion of privacy in public, at least when it applies to physical, public places, has gained more traction within the Chinese than the American public.

## ANONYMITY

Perhaps the first thing we might notice from the juxtaposition diagram to the right is that it seems slightly out of phase. The word pseudonymity appears in the top region of the top rectangle without any Chinese term in a corresponding position. In the lower portion of the rectangles, where one word, anonymity, appears in the top rectangle, two Chinese words, *wuming* (無名) and *niming* (匿名), appear (with *niming* perhaps a closer match to anonymity) in the bottom rectangle.

It is clear that in both China and the U.S., there has been a change in the nature of anonymity as human interaction shifts to the electronic, networked environment. The “no one knows you’re a dog” *New Yorker* cartoon epitomizes the early common wisdom on Internet interactions, that many of them were fundamentally untraceable. This apparent abundant anonymity led to its strong association with democracy (Akdeniz, 2002) but also to excesses such as “flaming” (Alonzo, 2004) where one or more discursive participants would engage in highly uncivil discourse, confident any improprieties or transgressions would have highly limited reputational fallout. Today, the sentiment appears close to reversing itself, where instead of everything we do online being anonymous, everything we do



appears to go into some massive digital dossier, forever haunting us with economic, political and social karma, both just and unjust (Solove, 2004; O'Harrow, 2006; Solove, 2007).

As I explained in chapter 2, personally identifiable information, while apparently simple in meaning on the surface, is a highly complex concept. It is often understood that anonymity is supposed to relate to some absolute condition of non-identifiability, while the word "pseudonym" is used to indicate the gray areas where one may be known or knowable to some, but not to all. Although it is easy to understand what we mean when we say a given piece of data is anonymous, it is more difficult to judge whether such a proposition is logically valid.

The contents of messages may, on their own, have enough information to allow particular individuals to be identified, as a number of Americans learned when AOL made a year of its search logs publicly available in an "anonymized" form. Individual records of particular search queries were identified with unique numbers, but no data linking these numbers to personal identifiers such as names or SSNs was released. Still, enough information was often available within the language of the search to trace it back to a particular individual. The *New York Times* published an article identifying one searcher, number 4417749, as Thelma Arnold:

... search by search, click by click, the identity of AOL user No. 4417749 became easier to discern. There are queries for "landscapers in Lilburn, Ga.," several people with the last name Arnold and "homes sold in shadow lake subdivision Gwinnett county Georgia."

It did not take much investigating to follow that data trail to Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga., frequently researches her friends' medical ailments and loves her three dogs. "Those are my searches," she said, after a reporter read part of the list to her (Barbaro & Zeller, 2006, paragraphs 3-4).

In the course of electronic transactions, an individual may be identified by a range of attributes including the IP address of the device they are using to access the network or by a more formal authentication scheme. Whether the IP address makes someone's transaction identifiable depends on the manner in which IP addresses are linked to individual identities in extant systems

of records. If your ISP stores your IP address with your personal information in a customer database, anyone with access to that database can use the IP address as a personal identifier.

In March of 2007, Google publicly announced a new policy to “anonymize” its search records after a period of 18-24 months.

When we implement this policy change in the coming months, we will continue to keep server log data (so that we can improve Google’s services and protect them from security and other abuses) - but will make this data much more anonymous, so that it can no longer be identified with individual users, after 18-24 months. (“Taking steps,” 2007, paragraph 1)

Google’s public announcement that it had made its search logs “more anonymous” provides a useful glimpse into just how confused the notion of anonymity has become. Google’s anonymization process consists of erasing a portion of the source IP address for the query and altering the unique cookie ID attached to the search in an unspecified way. Google admits, however, that this process does not guarantee that the government will not be able to identify a specific computer or user.

What is the relationship between anonymity and privacy? Is one necessary for the other? Anonymity, especially in the context of Internet interactions, does not necessarily lead to privacy. As Schneier (2007a) has pointed out, the contents of anonymous packets sent over the Internet can still be read by malicious individuals and institutions unless they are otherwise encrypted. U.S. government officials have begun to suggest citizens should give up their anonymity vis-à-vis the government while trusting them to respect their privacy (Single, 2007a). Although there was a predictable uproar in privacy circles, it remains to be seen whether the broader American public is paying much attention. Meanwhile, in China, there are growing signs that anonymity, at least among the young Internet generation, has a value that supersedes its role in the U.S..

In a November 2007 poll conducted by J. Walter Thompson, Chinese netizens were far more likely to claim that they experimented with alternate identities online than were their American counterparts. They also appeared to value online anonymity more, obviously a key resource in the negotiation of personal boundaries that may allow for such experimentation:

Chinese respondents were also more likely than Americans to say they have expressed personal opinions or written about themselves online (72% vs. 56%). And they have expressed themselves more strongly online than they generally do in person (52% vs. 43% of Americans).

That's largely because of the anonymity that the Internet offers, a key attraction for the Chinese. Chinese respondents were almost twice as likely as Americans to agree that it's good to be able to express honest opinions anonymously online (79% vs. 42%) and to agree that online they are free to do and say things they would not do or say offline (73% vs. 32%).

"One of the biggest differences between American and Chinese youth is in attitudes toward anonymity," says Doctoroff. "In the U.S., with its cult of celebrity, young Americans see the Internet as a way of getting known, of building their personal brand; many regard the Internet as a kind of personal broadcasting medium. But whereas publicizing your name, face and opinions is seen as a step toward success in the U.S., in China it has been a surefire way of veering into dangerous territory. So for young Chinese, the Internet is the ideal place to air opinions and hear what others think without crossing the line." ("China Leads the U.S.," Nov. 23, 2007, n.p.)

Although there is considerable appreciation for the role that anonymity can play in society (at least among the young), there is a very healthy respect for the importance of accountability and reputation, and recognition that anonymity can add unacceptable risk to certain kinds of social transactions. The public, for example, seems to have responded positively to the opening of the national identity registry database. Accessible via cell phone short messaging service and the Web, anyone residing in China can log in with a person's name and ID number to verify their identity. If the ID matches the provided name, the database sends back a photo of the ID holder to help verify that the ID is held by the authorized user ("China Provides," 2007). Angry Chinese blogger suggests that the reaction to the new system has been positive among a wide range of business owners such as hoteliers and store owners, but is marked by suspicion and concern within the "activist and industry insider" community ("Confirm a Friend," 2006).



## COLLECTIVE AND INDIVIDUAL ANONYMITY

Hertz (2001) suggests two possible Chinese translations for anonymity:

In the Shanghai Renmin Chubanshe English-Chinese dictionary, anonymity is translated either as *niming* (hidden or concealed name) or *wuming* (without a name, but also indefinable, indescribable). These two terms are generally used not as nouns but as adjectives, as in “an unknown hero” (*wuming de yinxiong*) or an “anonymous letter” (*niming xin*). Note that the two translations have very different connotations: in the first example, the anonymous (*wuming*) hero has been violently stripped of his . . . particular identity (name), literally and figuratively sacrificed to the collective cause; in the second example, the anonymous (*niming*) letter writer has chosen to conceal her identity, indeed her face, for reasons that are eminently personal, not collective. (p. 280)

While it is important and helpful to note the distinctions between *wuming* and *niming*, it is premature of Hertz to assume that *niming* could only be in the interest of the individual and not the collective. The increasing salience of *niming*, or online anonymity, can be understood as more than a simple increase in the valuation of individual rights and needs that has accompanied modernization and digitization.

## XIAMEN PX CHEMICAL PLANT PROTEST

If we consider a recent event of interest in Chinese history, the successful protest of more than a million anonymous citizens against a planned chemical plant, we can begin to get a sense of the complex ways that anonymity might mediate the relation between *gong* and *si*, (or perhaps even better, the tripartite relation between *guan*, *gong* and *si*). We can also begin to think about the often tenuous nature of anonymity, both as it relates to technology and social space, and its role as a resource when individuals find their interests in tension with those of the state. In the spring of 2007, citizens in the seaside city and special economic zone, Xiamen, began to become concerned over a new 11 billion Yuan (U.S. \$1.4 billion) industrial project in the city's Haicang district designed to produce large amounts of xylene.<sup>35</sup> Although the project had overwhelming

---

<sup>35</sup> According to the U.S. labor Department's *Occupational Safety and Health Guideline for Xylene*, "Chronic exposure to xylene may cause central nervous system depression, anemia, mucosal hemorrhage, bone marrow hyperplasia, liver enlargement, liver necrosis, and nephrosis [Clayton and Clayton 1981, p. 3295]."

support from the city government, citizens in Xiamen were able to make use of Internet bulletin boards, e-mail and short messaging services to organize a public protest of more than ten thousand people at the city center on June 1<sup>st</sup> and 2<sup>nd</sup>, leading to the temporary abandonment and eventual halting of the project there.

A few months after the protest, the city government announced draft rules banning anonymous Web postings for city residents (Dickie, 2007). The move caused considerable controversy and reignited the debate over the seemingly shelved national policy requiring mainland Chinese bloggers to register their real names.

It appears that the new regulation was a unilateral action by the city government, which stands to lose significant tax revenue from the lost project. Guangzhou city's *South Metropolis News* quoted He Bing of the China University of Political Science and Law in Beijing saying, "Only the National People's Congress has the right to legislate on this issue." It is also doubtful whether the city alone can enforce such a measure online, which also includes new rules for pre-publication vetting of content.

One could argue that Chinese citizens in Xiamen that day took advantage of their anonymity in online forums such as BBS and chat groups to engage in organizational actions which would otherwise be highly constrained. Although the individual actions were justified based on the way anonymity protected them from state harm, the result was the concerted voice of a collective *gong* that overpowered the more *si*-like *guan* (official) interests. It was this collective crowd of otherwise *wuming* (nameless) citizens out in public that electronic *niming* (concealed identity) made possible.

The Xiamen PX demonstration, perhaps, was dependent less on actual anonymity and more on perceived anonymity. Whether or not the initial organizers were truly anonymous as they

began to send out the short messages and BBS notices that would help bring millions to the streets, their perceived anonymity likely emboldened them to take the actions that quickly crystallized into a highly visible public. Those people who chose to take to the streets were videotaped and could easily be identified later, but the numbers being what they were nothing much could be done.

## CONCLUSION

One danger is that we remain satisfied with merely juxtaposing such concepts; the second is that we thereby remain in such an early stage of an intercultural dialogue, defined by what may only look like a common ground or an incompatible view - a common ground or incompatible view that in light of further dialogue, however, will dissolve into far more complex inter-relationships. (Capurro, 2006, p. 45)

A complex plural society will speak a complex plural language; or, rather, a plurality of specialized languages, each carrying its own biases as to the definition and distribution of authority, will be seen as converging to form a highly complex language, in which many paradigmatic structures exist simultaneously, debate goes on between them, individual terms and concepts migrate from one structure to another, altering some of their implications and retaining others. (Pocock, (1971), p. 221 in Rowe (1990), p. 324)

What might we gain by challenging the basic assumption that the conceptualization of “privacy” flows in one direction, from West to East? What insights might there be gained from understanding China’s contemporary and historical thinking on the matter, facilitating the “travel of words and ideas between languages” that Liu (1995) speaks of (above)? It should be clear after this brief exploration that questions about privacy can effectively be moved to an intercultural domain that benefits all participants while helping to build global schema of resistance (boundary resources) to extreme forms of institutional surveillance.

A great deal of both modern and traditional Chinese thought and culture is relevant to this struggle in Western discourse over how to define and value privacy. If neo-liberal arguments that privacy is merely instrumental to other individual and social goods such as security and prosperity continue to gain political legitimacy, basic individual and small group interests become

vulnerable in a way that may comprise the viability of future social systems. Aspects of Chinese thought and culture, including Confucianism and its more modern variant, Neo-Confucianism, may offer insight into how to make arguments that the loss of privacy would significantly impact the society level as well.

Any honest assessment of the “reasonable expectation” of privacy in China and the U.S. should find that the notion plays a role in both countries, and, more importantly, that this notion is in constant flux and is unlikely to serve as the basis for strong legal protection for privacy. Much might be made about the fact that the Chinese right to privacy is legally subordinated to the public interest. Nevertheless, few scholars in the West attempt to maintain that privacy trumps all other values. There appears to be room for a common, abstract notion of reasonable privacy as inherent in a continuously negotiated dialectic tension in information flow that forms the basis of more contextual, culturally embedded experiences.

The notion of territorial privacy is highly relevant to both the U.S. and the Chinese experience. While the U.S. legal system is dealing with an intensifying rupture in the link between territorial and information privacy first felt in the early 20<sup>th</sup> century, the Chinese have been adjusting to increases in real space that have been a major factor in increasing privacy expectations. Further, while the idea of privacy in public still has not been sanctioned within U.S. legal discourse, the Chinese public appears to have had at least some influence on the emergence of municipal CCTV surveillance laws.

The semantic link between the words *gong* and “public” to the notion of public opinion is not uniformly associated with physical public space such as a town square. In Chinese discourse, *gong* is often deployed to signal the abstract, non-spatial notion of society’s collective interests. The public-private distinction in Western discourse often includes spatial entailments (outside

and inside), making it generally less abstract than the *gong-si* opposition. Perhaps the disorientation relative to the public private distinction felt in Western discourse is not as acute in Chinese discourse, since the term is more abstract (protean) to begin with. Further, it appears that Chinese youth may value the new electronic domain of personal and social life to a greater degree than their American counterparts.

Chinese Internet and cell phone users are clearly concerned with the issue of spam and frustrated that individual companies can sell their addresses and phone numbers to other countries. It is probably far more likely for this public sentiment to translate into a nationwide law that significantly restricts the sharing of PII across private firms than it would be in the United States, in which business interests have a more direct claim on politics.

China does not share the U.S. tradition of politically neutral NGOs acting in the public interest, and is in fact only a few decades removed from the oppressive excesses and stifling mass surveillance programs of the Cultural Revolution, but the public today has begun to assert itself in significant ways. Since the September 11 terrorist attacks, Americans in general seem to be more aware of the tensions between security and privacy than their Chinese counterparts. More detailed study of demographic trends in both countries is needed to help envision more long-term scenarios. An important aspect of public sentiment to watch over time will be “trust in government.” In the United States, polls show that a large percentage of Americans lack even basic trust in their government. For example, a Scripps Howard/Ohio University poll conducted in the summer of 2006 found that more than one third of respondents believed “that federal officials assisted in the 9/11 terrorist attacks or took no action to stop them so the United States could go to war in the Middle East” (Hargrove, 2006). Would we find similar or greater numbers of basic distrust in China? This question is difficult to answer, as Chinese generally refrain from direct, public discursive attacks on the government for obvious reasons. Nevertheless, a number

of scholars have offered data suggesting that Chinese trust in government is quite strong in both urban and rural areas (Chen, 2004; Li, 2004; Wang, 2005; Fewsmith, 2007).

Whether or not it is possible for any individual to be truly anonymous when they engage in communication and information retrieval online is one of the “hard problems” of information science. Nevertheless, among young Chinese, the belief that these activities can be anonymous clearly has an impact on their willingness to engage in certain kinds of behavior. Further, it is quite clear that identification and authorization systems run by both public (state) and private entities, systems such as national ID cards, blogger real name registration, cookies, and RFID tags, have a great deal to do with the answer. The more people are required to use various forms of identification before acting (engaging in financial transactions, traveling, reading and sending e-mail) the more these actions are likely to involve the production of PII. In the next chapter, which looks at the state dossier system in China, I examine this interplay between state ID and record systems in detail.

## CHAPTER 6: CHINA CASE

The Chinese *dangan* (personal file) system of the mid 20<sup>th</sup> century was what one might call an “ideal form” of the state dossier system. That is, the dossier covered a significant percentage of the population (most urban residents,) and contained a wide range of detail, including the individual’s psychological profile, educational achievements, political attitude, and social network. The sites and logics of personal information production were strictly detailed and embedded in daily institutional practices, with little opportunity for resistance. This system, which I will describe in the first part of the chapter, did not focus on identification because it was built into the social environment and in little need of official attention. Since the *dangan* system was administered locally by intimate acquaintances of their subjects, identification was rarely a question. People’s lives in general were watched closely, not only during their working hours, but at home and in the local neighborhood. Privacy was in short supply and the notion of anonymity had little salience.

In the late 90s and into the 21<sup>st</sup> century, however, the production of dossiers has been undergoing a radical process of transformation. With China’s reform and opening process gaining momentum, the increasingly mobile labor pool has made official ID documentation much more important. And now with electronically mediated transactions growing rapidly online, networked communication ID technologies have become important as well. At the same time, as these new systems of ID have diffused into the social system, there have been important moments of resistance that were far less typical before. The sites and the logics of production are also not as clear, though there are certainly a number of signals that make it possible to draw a preliminary map.

In the Chinese case, the disaggregation of primary components of the state dossier system — ID technology and systems of records — makes less sense for what I will call the “traditional dossier system” that characterized the 1980s. Identification technology does become important in the late 1990s, as it plays a central role in enabling new sites and new logics of dossier production in the digital era. In this chapter, I first will describe the state dossier system as it existed in the 1980s and explore four primary sites of production — government departments, schools, work places, and local public security bureaus — each with their own slightly different but ultimately harmonious logics. Next, I describe three major transitional forces that have helped to revolutionize the production of the dossier: 1) *labor mobility*, 2) *globalization* and 3) *ICT modernization*. After reviewing these transitional forces, I will look more specifically at the current state of the two primary dossier system components, ID systems and systems of records. Finally, in the conclusion, I summarize the problem of the state dossier system in China today, in particular its unfinished, contingent nature.

## THE TRADITIONAL DOSSIER SYSTEM

Both the *hukou* and the *dangan* are distinct tools of the Chinese bureaucracy, but they were designed to operate at different levels of scale. The *hukou*, a system for registering both urban and rural households, has largely been a macroeconomic tool for distributing resources and controlling the population as a mass. The *dangan*, on the other hand, is a bureaucratic product designed to reflect the unique essence of individuals, making it easier for the state to locate and cultivate necessary human resources while quickly identifying and isolating political enemies. Both the *hukou* and the *dangan* involve the production of files containing PII, but the *dangan* has generally been far more detailed.



## HUKOU SYSTEM

According to Wang (2005), the Hukou system has traditionally had three primary functions: 1) distribution of resources and services to citizens; 2) the control of internal migration and 3) the monitoring and control of “targeted persons.” The salience of the term *hukou*, for the average Chinese has had little to do with dossiers. Rather, a *hukou* is a categorical designation which marks a major “class” division of society between rural and urban people. Chinese citizens with an urban *hukou* have had access to a wide range of social services and privileges not available to rural peasants.

The standard *hukou* contains seven categories of information: birth, death, personal data, family relations, migration in, migration out, and changes or corrections. This basic information is generated for every Chinese resident. This information is easily visible within the *hukou* booklet and thus accessible to the subjects. More extensive information is also generated by the local police officer for the *hukou dangan*, but this data is considered a state secret and is not accessible to the subject or any other unauthorized individuals. We will discuss this more extensive file below. For most residents, the *hukou dangan* contains little information other than that captured during the standard registration.

The *hukou*, for most of its history, was a paper booklet with several pages containing information on people within a given *hukou* unit — usually a family in urban areas or a village in rural areas. The first page contained biographic information on the “*hukou* holder,” the head of the family household or the village leader. Subsequent pages contained information on all other people within the household, including children. During this time, identification cards were of far less importance. Local *danwei* (work units) might issue their workers simple ID cards indicating their status as a worker, but there was no national standard and the cards had no certifying authority outside their originating work units.

In the early 60s, in the aftermath of Mao's failed Great Leap Forward, *hukou* became a key state tool for managing the influx of peasants from rural villages into cities. Peasants who attempted to live and work in the cities without state authorization would have to do so without access to the socialist safety net, the "iron rice bowl." *Hukou*-less migrant workers would have to live on the margins, with no access to medical care or education for their children, scraping out their living in the black market, thus lowering the incentive to migrate.

The *hukou* system has generally operated without significant legal oversight. There is no mention of the system in the state Constitution. It came into existence with the 1955 law, "The Regulation on Hukou Registration of the People's Republic of China," as the government's primary means for managing the distribution of resources. No other legislation was passed regarding the system until 1985, when the "Regulation on Residents Personal Identification Card in the People's Republic of China" outlined the new national ID system. Eighteen years later, the country's second generation national ID system was codified in the 2004 Law of Citizen Identification Cards. This was the first time that the *hukou* system was addressed in Chinese civil code. Prior to this, changes to the system were proclaimed by order of the State Council some 600 or more times between 1958 and 2005 (Wang, 2005).

Over the years, the central government has pushed reform of the *hukou* system that has tended to open up avenues for rural residents to move into the cities. Although some observers have suggested that China will soon eliminate the system entirely, such a move appears unlikely. While the state has decentralized decisions regarding urban migration to the cities themselves, it has centralized the monitoring and control of the "targeted population." The role of the *hukou* as the identification component of the modern state dossier system will be explored later in this chapter. First, however, I examine the traditional personal file system known as the *dangan*.

## TRADITIONAL SITES OF *DANGAN* PRODUCTION

In Chinese, the word *dangan* simply means “file.” Without additional linguistic differentiation it is often a source of confusion. During the peak of the state dossier system in the 80s, a person referring to his or her *dangan* would be generally understood to be referring to the comprehensive file about their life held by the personnel department at their local work unit (*danwei*). There are actually a large number of different types of *dangan*, some reflecting different chapters in an individual’s life and others part of distinct social groupings. To completely distinguish the personal dossier from any other type of file generated within bureaucratic processes, one can use the term *renshi dangan*, personnel file. Within the category of personnel file there are three large sub categories: the cadre dossier (*gangbu dangan*), the worker dossier (*gongren dangan*), and the student dossier (*xuesheng dangan*). The *hukou dangan*, the dossier maintained directly by *hukou* police, is only significant for a small sector of the population known as the “targeted people” (*zhongdian renkou*). Each of these four primary sites of dossier production is discussed below.

## CADRE DOSSIER SYSTEM

The dossier system has its origins in the more narrowly targeted dossier system for those individuals who were party members and directly employed by the government in a state or party organ: the cadre dossier system. The *dangan* system for cadres was a key bureaucratic tool during the fifties and sixties, enabling both the recruitment of talented individuals for key government posts and tight control over their political behavior. Government bureaucrats at the time were strongly convinced that thorough knowledge of the people, especially those people likely to become part of the communist project, was critical to the nation’s development:

[We] have to examine whether or not one has unlimited loyalty to the party and people and one’s political and historical records, ideology, personality, and attitude toward study. [We] have to examine them regularly. Only when we have made a detailed

examination of each cadre's political history, political conditions, political quality, ideology, work style, work performance, and ability in a systematic way, can we systematically understand cadres, correctly recruit, and use them. (Lee, 1990, p. 330)

Although the cadre *dangan* has directly impacted only a small sector of the population, it is the most fully developed system upon which systems for the general population have been based. The file has traditionally been a physical set of documents intended to follow the individual around throughout the life career:

The principal is not to spread the material from the file over several different units; it is assumed that this would prevent the administration from getting a correct picture of a person's all-round situation. (Bakken, 2000, pp. 290-1)

The *dangan* file consisted of a mixture of records produced by the subject himself, the subject's peers, the subject's superiors, and, at times, special investigators carrying out the directives of a political clampdown campaign. According to Lee (1991), the dossier subject was expected to fill out a number of key forms along with a more free-form autobiography. Although there has been some variation across state and party organs, key forms included the "Summary Career History," "Promotion to Cadre" (if newly appointed) and "Application for Party membership." General categories of information on these forms included basic registration information seen on any standard *hukou* form, detailed family background, including the occupations of family members prior to the revolution and current economic situation, names and employment details of close friends and associates, and information about prior arrests, jailing, or executions of key family members. In addition, registrants were asked to provide specific information about when and how they became a party member and whether or not the spouse was a party member. The autobiography, chiefly an exposition of the subject's political life, including participation in demonstrations or associations from age seven on, provided an opportunity for the subject to provide context or additional information not easily included in the basic forms. Most cadres had a single physical file which was held by the personnel department above them. Cadres

of greater importance had two versions: a highly detailed file, with very tight access restrictions, and a digest version, for which there was wider, but still restricted access.

In addition to the volume of information generated during a cadre's registration for a new position, a key part of the dossier production cycle was the year end appraisal meeting, in which the subject's performance as a cadre was reviewed in detail. Chow (1993) describes the meeting:

During the year end appraisal meeting, each cadre is to prepare and orally present a written report of his work. Contained in the report are a descriptive list of the tasks being accomplished, an account of accomplished tasks, and plans for performance improvement. After the oral presentation, the "mass" is to assess accomplishments and/or failures, including those which are not mentioned in the report; such assessment is to be made based on the job description of the position occupied by the cadre. The "mass" will also give suggestions for performance improvement. After group discussion, leading cadres are to draft a revised report, which includes the original self-appraisal and those additional comments from the "mass." The "mass" will then consider and endorse the final report to be signed by the cadre and the leading cadre. The report is to be filed in the cadre's dossier. (p. 112)

Key to understand here is that the subject was a direct participant in the production process and produced what was in essence a draft of the file that was to be placed in the dossier. Although they were not allowed to view the contents of their dossier, they often had a pretty good idea of its contents. Those cadres who fit well into the system and were liked by both their peers and superiors tended to have a sense of control over the dossier that more marginal cadres did not.

Cadres who saw the *dangan* as threatening would be in greatest danger, not during the regular, periodical evaluation process, but during another key, but irregular moment of dossier record production: the political campaign. These campaigns, used by Mao to ensure that all party and state organs held to the "class line," ended with purges of large number of party members who were viewed as obstacles to the communist project.

During a campaign, the personnel bureau or organizational department holding the dossiers would go through each file carefully, looking for evidence that the subject had

deliberately falsified material that could hide evidence of political misdeeds or associations with other “black marked” individuals. Dossier administrators focused on the autobiography section and the numerous supplements the subject provided to it over the course of his life, looking for internal inconsistencies. If an important discrepancy was found, special investigative teams could be dispatched by the party committee to investigate more thoroughly, including interviews with the subject’s associates. The process ended in a formal report added to the dossier, at best noting the discrepancy, and at worst categorizing the subject as a target for punishment, producing a “black mark” in the dossier that could impact the subject for the rest of his life.

The handling of dossier files during the course of these investigations, described by Lee (1991) helps illustrate the degree to which the party sought to maintain the file’s integrity:

Investigators are allowed to see dossiers of those specified by the letter only in the designated dossier room. No mechanical duplication of a dossier is allowed except for a simplified version of the dossier. When part of a dossier is copied, it is verbatim; no summarizing or paraphrasing is allowed. The person in charge of the dossier must authenticate every page copied in the entire package.

Control over copied materials is strict because they can enter the dossiers of others as supporting evidence. To ensure proper control, the regime authorized each unit maintaining dossiers to set up more detailed regulations. As for lending dossiers, “as a rule, a dossier cannot be checked out. But under special circumstances, it can be lent with approval [of the party committee.] However, lending should follow strict registration, and those borrowed should be returned within the due date.” (pp. 337-8)

In other areas of society, including the labor and education sectors, files on general individuals were limited and narrow in scope until 1956, when the cadre *dangan* system was standardized and unified nationally. As part of this process, other sectors of society began to follow this model, extending the topical coverage of their files to include more about their state of mind and attitudes toward the political system:

After 1956, this political/ideological component of the worker’s file became the “lifeblood” of enterprise management work, for it was argued that it was not enough to understand only the individual worker’s circumstance; knowledge of the influence of

family members, as well as members of the community, upon the workers was also needed. (Dutton, 1992, p. 226)

#### EDUCATION DOSSIER SYSTEM

Since 1956, a Chinese citizen's first experience with the dossier system has generally been through school. The primary person responsible for managing the production of *dangan* material within the educational system is the student's teacher. In the process, however, both the student and their parents are heavily involved. The primary document produced by the school teacher is the student evaluation report written every school term. A lot of input for this report comes from a process known as the "contact transmission record," a written document intended to bridge communication between the parents, the school, and the student:

The parents' meetings should continue at regular intervals, and the already widespread practice of home visits by the teacher should be upheld. The contract transmission record should ambulate between school and home every week. It should carry notes on the students' moral behaviour, the rules of study, attendance record, test record, level of hygiene, delivering of homework, etc. Students themselves should bring the book home every Saturday; parents should use the weekend to go through teachers' evaluations, and carefully write down the students' *biaoxian* at home; each Monday the students should bring the record back to school. The teacher could then inspect it, and direct education towards any specific problems. This 'connection record' (*guanxibu*), the home visits, and the parents' meeting (*jiachang hui*), used together, could gather the best information possible about the students. (Bakken, 2000, p. 277)

It is notable that their early experience with the system is positive; the file is seen primarily as a tool for the encouragement of the student's development. According to Bakken (2000), teachers saw the program largely as one of "constructive assessments intended for encouragement" (p. 293). The character of the *dangan* appears to shift more towards discipline and away from cultivation as the individual moves higher in educational institutions and on into a chosen profession, but the file administrator is still someone who interacts with the individual on a regular basis. Although the individual is not allowed to see their file, they remain an intimate part of the process.

### WORKPLACE *DANGAN* SYSTEM

When a student moves from the educational system to their first job, the personnel file is sent from the school to the new place of work, where the file becomes the responsibility of the work unit's party secretary. As in the cadre system, strict secrecy of the files is maintained. The *dangan* is kept in a special room to which only authorized party members have access.

The mechanism for the production of dossier material and their use follow closely the model of the cadre system. The person primarily responsible for dossier production is the worker's production group leader. The political logic of the worker *dangan*, however, appears to lean more toward identifying political enemies than cultivating their spiritual consciousness. Since workers are not expected to go far up the political chain of command, attention tends to focus on those likely to be sources of dissent.

Study reports are regularly filled out by production group leaders based on the results of political study sessions. In addition, group leaders continually give oral "small reports" (*xiaobao*) on the situation in their groups, including the disposition of individual workers. It is likely to be reported if, during political study or the work day, a worker offers a heterodox opinion that requires criticism or reflects an unyielding attitude with regard to party policy. The report makes its way up the party hierarchy and will sometimes come to rest in the personnel department, where it will become part of the worker's permanent record if the person in charge judges the matter to be serious. (Walder, 1987, p. 68)

The worker's *dangan* is the central document their superiors consult when considering workers for promotion, punishment for transgressions, or the provision of housing assignments. As is the case with the cadre *dangan* system, elements within these files can also make them targets of political campaigns. As a result, workers can become very concerned about possible black marks that could affect their and their family's futures. A major effect of this is the depoliticization of workers outside the approved party structure:

The most important consequence of this system of political surveillance and control is that it makes it almost impossible for workers to organize themselves to formulate their own proposals and agendas of issues outside of party auspices and without the organizations knowledge. The communication among workers so critical for effective



political action cannot take place without the Party detecting it and applying sanctions to those involved. One activity that has been treated with consistent severity in China is political organization outside the Party; it is by definition counter-revolutionary. Where this system of surveillance is intact, workers are demobilized as a political force. (Walder, 1987, p. 69)

During the peak of the traditional dossier system, the dossier created a comprehensive, imposing data shadow for each and every urban resident, from their early days in school until the end of their productive life. For most of this population, these two sites, education and work, were the exclusive locations where the production of dossier materials took place. Because the file existed in a singular location (excluding the police copy) and was managed on the basis of direct, personal contact with the subject, there was a strong belief among administrators that the file represented an objective view of the person in question:

Since the file is based on the objective evaluation process, it is also held that 'the personnel file ... is an objective report of a person's objective aspects or features'. This is to apply whether the file concerns cadres, workers, or other individuals; the objective features to be reported are the individual's moral, political, intellectual, and work abilities, rewards and punishments, etc. It is explained that the file represents a full reflection of a person's past and present situation; in particular, it is emphasized that the file is 'a proof of the education a person has got under the leadership of the Party'. The file objectively measures the distance from the exemplary and objective norm for each individual. (Bakken, 2000, pp. 299-300)

This distance from the exemplary, frozen within each instance of the file, was the basis upon which individual were to develop their self-improvement. In a person's early experience with the *dangan*, he she would see the file more as a tool of education and betterment than as a tool of strict social control, but always in conjunction with the intervention of a higher authority. The teacher, for example, can exercise their own discretion as to whether a particular problematic episode, such as speaking out of turn in class, makes its way to the permanent file. They also work regularly with the parents and the students themselves in conducting their evaluations, which ultimately lead to the production of a formal report.

Throughout the majority of modern Chinese history, access to the dossier has been highly restricted, with the information inside classified as a state secret:

When critics of the regime demanded public access to personnel dossiers, the regime gave three reasons for their being kept secret. First, an individual's privacy must be protected from other individuals (but not from the state). Second, dossiers include facts that have been verified as well as suspicions, rumors, and other pieces of potentially damaging, but unconfirmed, information that should certainly not be made public. Third, a dossier's confidentiality prevents unnecessary disharmony among the people. (Lee, 1990, p. 332)

#### POLICE *DANGAN* SYSTEM

For most Chinese citizens, the local public security bureau has not been a significant site for the production of dossier material. All citizens must register with the local office at birth, and urban residents have special *hukou* police assigned to them, charged with maintaining detailed files. In practice, however, *hukou* police keep active files on only a very small percentage of citizens.

As of 2006, more than 300,000 specialized *hukou* police officers were assigned to geographic zones of from 500 to 1000 households, or as many as 2,500 people. These special officers were given the responsibility collecting, updating and verifying the *hukou* information for all people within their zone. The information gathering process was guided by a standard form with eight categories:

... basic information (the information on the *hukou* registration form); current behaviour including political activities; family and personal financial status and life style; personal friends and relations (including love relations); physical features including body size and body shape; usage of accent and slang; personal character and hobbies; and daily associations and other “consequential” past activities. (Wang, 2004, pp. 124-5)

In addition to collecting information to fill in the public security file, *hukou* police have also maintained copies of their people's school and work dossiers. Given the size of their domain and their limited resources, *hukou* police were simply unable to maintain highly detailed data for every resident. A kind of “triage” system emerged where their attention and dossier production

activities were focused on a small subset of the people in their zone, the “targeted people,” with the remainder largely free of this documentary coverage.

It is difficult to say with certainty just how many Chinese citizens are targeted in this way, as the information is considered a state secret. In March 1985, the Ministry of Public Security issued “Regulations on the Management of Targeted People” classifying them into six major categories: 1) those under suspicion for counterrevolutionary activities; 2) those under suspicion for ordinary criminal activities; 3) those suspected of disturbing social order; 4) “risky elements” who might use violence in times of civil unrest; 5) those under control (by the public security bureau), who have been deprived of political rights, who are out of prison on parole, who are serving a sentence outside of prison, who are under house arrest, or who are on bail awaiting trial, and 6) those who, within the past three years, have been released from prison or RTL (Reform Through Labor).

Data collected by the Duihua foundation, a non-profit group dedicated to protecting human rights in the U.S. and China, shows that Mohe County, an area of Heilongjiang Province near the Russian border with a population of roughly 75,000, had between 6 and 84 people targeted over the course of the 1980s, or a maximum of .11% of the population. According to Wang (2005), a Tianjin city police station with 35,000 residents had a list of 247 targeted people in 1998, or .7% of the population, and a medium sized city in Henan province had 22,000 of its 1.1 million population listed as targeted, or 2%.

The group of people involved in the production of records for the *hukou* police targeted *dangan* is broader, a social circle not as intimately involved with the subjects than in the education and work sites. In order to gather the necessary information, *hukou* police make extensive use of informants within the local communities. Prior to Deng Xiaoping’s economic

liberation, finding informants with useful intelligence on local residents was a fairly straightforward process. Local heads of neighborhood committees, often gossipy older women, watched and listened to their people carefully and had much to tell the *hukou* police. What Wang (2005) calls a “deep and extensive political cynicism among the citizens” (p. 125) has grown in the 90s and into the 21<sup>st</sup> century, making the average urban citizen far less likely to willingly act as the “eyes and ears of public security” (*zhi'an ermu*). To make up for this change in the social landscape, police began to shift from using volunteer informants to paying them directly, often using ex-criminals who might have ins to the targeted social networks (Dutton, 2005).

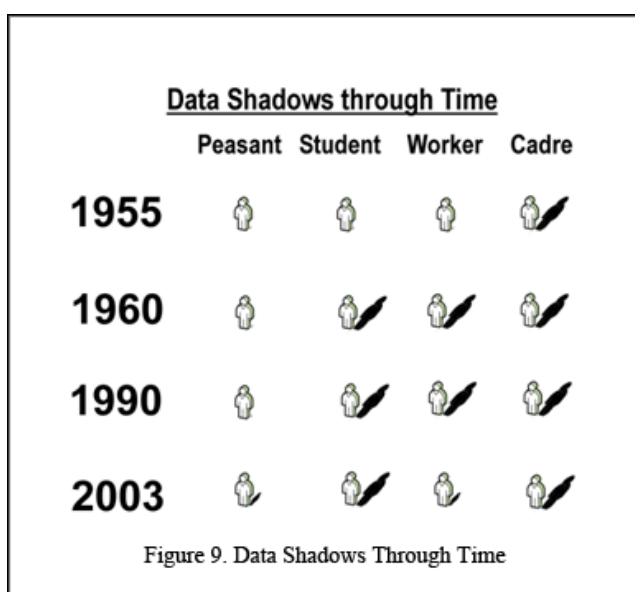
Local public security bureaus are directed by the central government to target specific people, although they may also add people who come to light during local policing activities. For targeted people, the police officer must fill out all eight categories of the police form and fulfill additional information requests from the central government. In addition, they are expected to surveill and interact with the targeted person on a regular basis:

... the police are instructed to monitor the targeted people openly and secretly as closely as possible, review their cases and “educate” them as necessary, and detain them at the earliest warning signs. Often, especially during periodical national or regional yanda (strike hard against crime) or saohai (sweeping organized crime) campaigns, the targeted people, together with undocumented “floating” people, are preemptively detained and interrogated without evidence of criminal activities. (p. 126)

People who fall into this category of “targeted person” clearly exist as second class citizens. The far majority of the urban population, however, has not traditionally been subject to this process of dossier production. For the average person, their police *hukou* file “may include only a copy of his or her *hukou* registration application....” (Keane, 2005, p. 217).

*DANGAN* “DATA SHADOW” BY PERSON TYPE

The size of the data shadow, cast in the traditional *dangan*, has varied considerably, both over time and according to one's position in society. During the first ten years of the communist regime, only state cadres, personnel working directly within state and party organs, were subject to the national dossier system. By the late fifties, most urban residents, from factory workers to street sweepers, were in the shadow of an extensive and momentous personal file, beginning with



their time in secondary school. The size of this shadow, however, varied considerably according to one's social position and type of employment. A decade after Deng Xiaoping's urban economic reforms, many urban residents found themselves free of the *dangan* shadow (at least once they left school) while peasants have been largely independent of the dossier system for

nearly all of the country's 60-year history. As the Chinese dossier system is in the midst of a rapid period of evolution and change, the size of the data shadow for people from all walks of life is again in flux.

### THREE MAJOR FACTORS IN THE TRANSITION OF CHINESE SYSTEM

Although China has had a nearly prototypical state dossier system for much of its modern history, both the logic and sites of file production are undergoing a radical transformation which has at least temporarily destabilized the system. So far, for the average Chinese citizen of the 21<sup>st</sup> century, the government dossier is less oppressive a notion than it was for citizens of the prior century. Whether or not this destabilization is temporary or the harbinger of a deeper shift in the

country's socio-political environment will in large part be determined over the course of the next few years.

There are at least three significant changes in China's social environment that have led to this shift: 1) the increasing mobility of the working class; 2) growing integration into the global economy and 3) the diffusion of personal computers and network communication technology. Although these three changes clearly have their own interdependencies, using these three categories of change makes it easier to outline a broader narrative of this radical shift. Again, both the sites of production, the physical and institutional locations where dossier files are being produced, and the logic of production, the schematized processes which generate and use the data, have changed dramatically over the past three decades, and, in fact, are still changing.

#### FACTOR 1: LABOR MOBILITY

The growing diversification of China's economic landscape with private and other non-state businesses and parallel reduction in constraints on internal migration have completely disrupted the standard process of dossier production for a growing percentage of Chinese citizens. While the production of information for the educational portion of one's *dangan* does not appear to have changed significantly, its importance in the world of work has been reduced dramatically. Once they go into employment, workers in state firms can expect their *dangan* to remain a central document determining their professional success. For government cadres, the document is of extreme importance. For those who work in the private sector, however, active maintenance of the *dangan* file appears to cease. Private firms are not required to receive or maintain the *dangan* for their new employees. Workers in foreign corporations send their sealed *dangan* file to the Ministry of Foreign Trade while those working for domestic firms send them on to the Ministry of Commerce.

The job of guarding files for people employed in the private sector has been contracted out. In the capital, the files of most privately employed workers are guarded by the Beijing Talent Centre, which is housed inside a former concubines' compound at the Forbidden City. Wu Yong, a senior manager there, calls the centre a "service business". The Talent Centre lacks the power of a party chief to annotate people's files, and merely has them for safekeeping. ("X-files," 1998)

We cannot assume that dossiers are no longer maintained on individuals in the private sector, just that the method of administration has changed. It is likely that *dangan* are forwarded and then digitized, where they become the basis for new virtual dossier to replace them.

A significant bureaucratic response to the increase in worker mobility was the institution of a national ID card. Prior to the issuance of the national ID card, Chinese citizens had to rely on letters of introduction from former employers and non-standard IDs that were easily forged. To identify people, the Chinese state relied largely on the local context. The person's school or work unit administrators knew them by face, so this rarely became an issue. As state administrative agents increasingly encountered people with which they had no prior interaction, the importance of authentic ID documents started to grow.

## FACTOR 2: GLOBAL ECONOMIC INTEGRATION

China's interest in opening to the world has been clear since party chairman Deng initiated the Four Modernizations in 1978. Part of the reform and opening process has been the opening of domestic markets to foreign players, the marketing of Chinese goods on the world stage, and the formal entry of China into the World Trade Organization. This integration has brought new logics to dossier production that flow from global models of risk management. Global, financial risk schema have encouraged an entirely new level of financial records production, while a growing number of private institutions are learning the value (both in use and exchange) of records of personal information. At the same time, foreign companies hire Chinese workers with no knowledge or interest in the traditional practice of the *dangan*. They still

maintain personnel records that may end up within the dossier system, but the logic of production there is far different than that of the 1980s communist party work unit.

International standards are also beginning to have an impact on the configuration of China's current state dossier system. Within the domain of identity systems, for example, China was pressured to produce passports for its citizens with an embedded RFID chip. The U.S. threatened China with a revocation of visa waiver status for travelers who came to the U.S. without RFID chips embedded in their passports. The process of dossier production is no longer entirely within China's control. In some cases, the government must request that private, foreign institutions provide records in which it has an interest, with at least the possibility of a "no" answer.

### FACTOR 3: ICT MODERNIZATION

Over the past several decades, the Chinese government has overseen the rapid modernization of its telecommunication infrastructure, nationwide diffusion of personal computers and cell phones, and adoption of electronic communication and record storage within all levels of government, commercial markets and increasingly among the general public.<sup>36</sup> The modernization has been impressive not only in scale but in pace. Since former party chairman Deng Xiaoping's call to open and modernize the country in 1978, China has been on a path toward modernization that has only been accelerating in recent years.

In the first fifteen years of modernization under reformist Deng, national telephone penetration had risen from roughly 0.4 per hundred in 1978 to 2.2 in 1993. The Chinese

---

<sup>36</sup> Although it would be possible to consider the diffusion of telecommunications technology and China's integration into the global system to be so intertwined as to be analytically inseparable, there is an important reason for separating them here. In focusing on technology, the emphasis is on changes to the dossier system enabled and catalyzed by the specific technological affordances of electronic networked communication and storage. One of the affordances of this new technology is the rapid influx of information China begins to absorb as it becomes more integrated with the global system.



government invested more than \$50 billion into improving telecommunications infrastructure, helping to boost the penetration of fixed line phones to over 20 per cent by the year 2000. With an additional 5-year commitment of \$120 billion announced by the MII in 2001 (“China to Pour, “ 2001), fixed line penetration has continued to grow, now hovering at close to 30% nationally. Soon after fixed line build out gained momentum, cellular phone penetration began to surge as well, passing fixed line penetration, with over 40% nationally as of early 2008 (Hanlon, 2008). The number of personal computers in use in China rose more than two orders of magnitude between 1990 and 2005, from just 4 for every 10,000 to 4.05 per 100 people in 2005 (“ADB Country Partnership,” 2008). More than 40 million PCs were sold in China in 2008 (Chao, 2009). Similarly, the number of Internet users in China has risen from 620,000 in 1997, to 22 million in 2001, to more than 300 million in 2009.

China’s technological modernization has been achieved via a combination of policies, including government funded programs, opportunities for foreign investment and technology transfer, and the cultivation of its own indigenous telecom and computing industry. In the past two decades, formal government programs for improving China’s communication capacity have included the Golden Projects, officially announced in 1993, Government Online, launched in 1999, and the comprehensive e-government initiative outlined by the State Council in 2002.

This process has not always been firmly in the grasp of the central government. The achievement has been much like rolling a bolder down hill; the initial force necessary to get things moving has unleashed a gathering momentum that the state can, at best, only nudge in certain directions. China’s leaders have been aware of the potentially disabling potential of ICTs since at least 1989, when the fax machines and electronic BBSs helped bring the clash between new media savvy pro democracy students and the Party to a violent conclusion. This has not slowed their enthusiasm for modernization, in part because the very same new media explosion

that caused them to lose control in those early days of June enabled them to identify and apprehend many of the students who defied orders to disperse.

The video cameras installed for traffic monitoring in the center of the city proved particularly useful. The definitive account of the whole event is in the hands of the Bureau of Public Safety. The operators of these remote-controlled cameras could pan and zoom in on the faces and actions of individuals in the square and environs. Being CCD-type cameras, they even work in very low light. Still frames of the faces of prominent activists in the square also turned up on television, broadcast all over the country to catch movement organizers on the lamb. (Wark, 1994, p. 131)

In the 20 years since Tiananmen, there has been an ongoing tension between the state's view of ICT as powerful tools of purely economic liberalization and their role as "technologies of freedom" affording new opportunities for human association and social innovations outside of state guidance. More recently, scholars have argued that cyberspace can support authoritarian or even totalitarian forms of government at least as well as it can facilitate democracy and the spread of human rights (Boas & Kalathil, 2003).

China's Golden Shield project, formally initiated by the State Planning Commission and Ministry of Public Security in July of 2001, can be understood in part as the state's focused expression of this tension: the state's collective effort to ensure that the ICT revolution remains in its control. The official goal of Golden Shield was "the adoption of advanced ICTs to strengthen central police control, responsiveness, and crime combating capacity, so as to improve the efficiency and effectiveness of public security work" (Qiu & Hachigian, 2004, p. 17). The project was designed to be implemented in two phases, with Phase One (2002-2004) focusing on building infrastructure and a common operation platform, and Phase Two (2005-2006) emphasizing the development of applications.

Golden Shield is an umbrella term for a number of interrelated initiatives, from the electronic networking of local and provincial ministries of public security, to the monitoring and control of Internet information flows, to the digitization of the *hukou* residential card and many

other projects. Of most relevance to this dissertation is how, as part of the Golden Shield project, the Ministry of Public Security is attempting to move the traditional dossier system into digital form, a plan it first formally announced in 2000:

The MPS announced last year that within three years it would have created a nationwide computerized database containing personal details and ID numbers for every adult in the country. In the past the Chinese government has kept a cumulative file (called the *dangan*) on every individual's performance and attitudes from kindergarten, and throughout adult employment. This information will now be digitized and Chinese citizens will be issued new, second-generation identification cards that will contain their *dangan* on an embedded microchip. Currently, Chinese ID cards consist of a laminated paper card featuring a person's name, photo, birthday and ID number.... The second generation smart card is likely to be a "proximity card" — in other words it can be scanned instantly, from several feet away, without the subject necessarily being aware that he or she is being identified. (Walton, 2001, p. 19)

The focus of attention within western academic and mass media literature has been the Internet censorship initiative, a bias which has become so pronounced that the term "great firewall of China" has, incorrectly, become virtually equated with the "Golden Shield."<sup>37</sup> The Chinese government's ongoing and evolving efforts to block unwanted information from flowing into or within its borders certainly distinguish it from the U.S. state, which does not attempt to interfere significantly with data flows. As we will see, other aspects of the Golden Shield program with more direct parallels to our study of dossier systems largely mirror similar policy efforts in the U.S.

The Golden Shield project is clearly very important to China's central government. The size of China's overall surveillance market, estimated at \$500 million in 2003, is projected to exceed \$40 billion by 2010. (Bradsher, 2007a) In 2005 alone, \$1 billion was invested by the Ministry of Public Security ("China Public Security and Surveillance," 2007). This is clearly a significant portion of government expenditure on ICT modernization which may continue to grow in the next several years. Nevertheless, it is important to understand that the state has modernized

---

<sup>37</sup> See, for example, [http://www.wired.com/politics/security/magazine/15-11/ff\\_chinafirewall](http://www.wired.com/politics/security/magazine/15-11/ff_chinafirewall)

telecommunications and accelerated the diffusion of ICTs primarily for two reasons: to boost economic development and improve government administration. These have been and continue to be the driving factors of modernization. This fact can often get overlooked in research that focuses on the Orwellian frame:

In spite of the overwhelming investment that China was making in building infrastructure, it seemed that only business analysts were impressed. Academics tended to focus solely on the way in which China attempted to control the internet at the individual user level. A survey of the published literature on China and the Internet concluded that an overwhelming number of studies sought to analyse the government's attempt to control the internet over Internet dissidents and cybercitizen's use of the resources of the web (Kluver and Chen 2003). The common picture that emerges is of the government trying to hold back a wave of political dissent against the authoritarian government, while attempting to use the Internet primarily for economic benefit (Boas and Kalathil 2003; Chase and Mulvenon 2002). This view is common not only in academic research, but also is especially pronounced in journalistic coverage of the Chinese Internet (McMillan and Hwang 2002). (Kluver, 2005, p. 83)

While informatization may help the central government to vastly increase its authority, the jury is still out. It would be a mistake to see China's continuing support of cyber-development as driven primarily by the desire to monitor and control the populous. This is an ongoing struggle whose outcome is highly contingent. In the rest of the chapter, we examine this struggle more closely, first considering the emergence of new identity systems and then the rapid growth in digital systems of records.

## ID SYSTEMS

Identification technology was not a particularly salient component of China's traditional dossier system because it was produced locally and participants tended to know each other quite well. As the urban population became more mobile, however, it became more and more important to develop a nationally standardized document to attest to identity. The first document was in low-tech paper form. Not only was the original ID easy to forge, but administrators had not even fully thought out the necessities for a unique numbering system, leaving close to a million people

across the country with duplicate ID numbers. Over the past several years China has engineered a major upgrade of the national ID card system and is now focusing its attention on expanding its online ID systems. In this section I will discuss the first national ID card, the second generation ID card, and finally, state efforts to implement comprehensive virtual ID systems online.

#### FIRST NATIONAL ID CARD

The State Council decree to establish a national ID card was announced in the *People's Daily* on April 7, 1984. "Personal identity cards are extremely necessary to tighten social security, to uncover, control and smash every type of serious criminal activity, to protect the well-being of the state and the people and safeguard the socialist modernizations," the announcement said. Highlighting the benefits to be expected by citizens from the new ID initiative, the announcement stated "citizens will find it more convenient to handle legal matters, register to vote, take college entrance examinations, seek employment, collect parcels or send remittances by mail, get medical care, travel and buy train, boat or air tickets" (Bradley, 1984, n.p.). The first step in this project, detailed in the "Trial regulations for identification cards for citizens of the PRC" was to establish a pilot ID card program in Beijing and to use that experience to draft a formal national ID law.

The following year, Liu Fuzhi, head of the Ministry of Public Security, explained to the *Xinhua* daily news service why a new system of identification was so important to the country's development:

For the sake of people's own convenience and to protect their legitimate rights and interests more effectively, the issue of uniform, legally valid citizens' identification cards by the state is essential. With this legal document, which is easy to carry, all a citizen needs to do is to show it whenever his identity has to be proven. Not only will the people benefit from the convenience, various departments concerned can also simplify formalities and improve their efficiency.

After adopting the citizens' identification card system and when our citizens have been issued uniform identification cards, management can be efficiently organised, social stability can be better maintained, the discovery, control and punishment of all types of criminals who have mingled among the people will become more effective and the safety of the state and the people as well as socialist modernisation can thus be safeguarded. ("Minister of Public Security Explains Need for Identity Cards," 1985, n.p.)

Draft regulations for the national ID card were adopted by the Standing Committee on September 6, 1985. Detailed rules for implementation of the regulations on residents' identification cards were passed by the Standing Committee a year later on November 3, 1986 and were officially promulgated by the Ministry of Public Security on the 28<sup>th</sup> of November. These detailed regulations included a specific listing of the situations and locales citizens would be expected to present their card:

(1) registering as a voter; (2) registering one's residence; (3) signing on for military service; (4) registering one's marriage; (5) enrolling at a school or taking up employment; (6) handling notarization matters; (7) going to controlled border areas; (8) carrying out exit formalities; (9) taking part in litigation; (10) applying for a motor vehicle driver's license, a ship navigator's license, and a non-motor vehicle driver's license; (11) applying for a license for operating an individual business; (12) handling individual credit loan matters; (13) taking part in social insurance and drawing social relief funds; (14) going through the formalities for boarding a civil aircraft; (15) registering at a hotel; (16) withdrawing remittances and claiming mail; (17) consigning articles for sale on commission; and (18) dealing with other matters.

The ID numbers associated with the original ID cards were not controlled at the central government level, leading to duplicate ID numbers among what some estimate to be more than a million people ("Overlapped ID numbers," 2005). ID cards were printed paper stock and very easy to forge. Identity theft and fraud became an increasingly common occurrence in the urban areas.

In 1999, the State Council issued the "Decision on Implementing a Citizen Number System" calling for every Chinese citizen to have a unique, unchanging, lifelong citizen identity number (CIN). The CIN is an eighteen digit number consisting of four blocks. The first block, six digits, indicates the administrative region for the *hukou*, which may range from a small

neighborhood in a small city to an entire town in the rural areas. The second block, eight digits, encodes the individual's birth date. The third block, three digits, is a "sequence number" used to distinguish those born on the same day in the same region. Finally, the last digit is a verification number used to check the validity of the number and card (Keane, 2005). The new, second generation card, described later in this section, took advantage of the CIN and included technology, RFID, to reduce the possibility for ID fraud.

The Chinese government continued to push the use of the national ID card. In January 1993, a circular from the Ministry of Public Security and thirteen other government departments underlined the importance of using the ID and the ID number when consulting or generating information about individual citizens:

The resident identification card is an official state document for certifying the identity of individual citizens. Departments should instruct their subordinate enterprises and institutions to formulate, institute or amplify the necessary rules and regulations in the light of the characteristics of their functions. They should check citizens' resident identification cards when the latter go through procedures in their political, legal, economic and social activities relating to their rights and obligations as citizens; and make the checking of resident identification cards an institutional and standardized system.

The circular asks all departments to use the data on the citizen's resident identification card - such as name, sex, nationality, date of birth - in their vocational work, in the issuance and registration of relevant documents, registers, certificates, forms, bills, instruments and cards relating to citizens' rights and interests. ("Identification: Ministries Seek," 1993)

A few months later, however, an incident in the city of Guangzhou involving the death of young migrant worker Sun Zhigang while in police custody would spark a public outcry against police treatment of citizens found out in public without proper documentation. In March 2003, Sun was jailed for not having his "temporary residence permit" and later died after a brutal beating in police custody. Hard hitting investigative reporting by the city's *Southern Metropolis Journal* was distributed widely on the Internet and resulted in the case becoming the focus of public attention ("84 Days," 2003). In the wake of the scandal, the central government was forced

to transform migrant detention centers like the one where Sun had been mistreated into voluntary service centers, while at the same time abolishing the temporary residence permit requirement that had been present in Chinese law for 20 years. Although the government later reintroduced the permit system, citing the need to manage the migrant worker problem, there continue to be active calls for the abolishment of the system, and the topic is considered fair game in the media (Qiang, 2006). In the months following this event, the government was forced to take a more conciliatory approach and rearticulate the rights of Chinese citizens surrounding their use of the cards. Some of these changes are reflected in the new, 2003 “Law on ID cards,” covered in the following section.

#### NEW EMPHASIS ON IDENTIFICATION: THE SECOND GENERATION ID CARD

China’s “second generation” national ID card was the culmination of a number of trends, the answer to a range of policy problems that the original national ID card had only partially solved. The first national ID card was instituted at the leading edge of Deng’s urban economic reforms and made possible rapid, short term increases in the mobility of the labor class. The second generation card was deployed within a different political, economic and technological environment. Deng’s reforms have helped to spur three decades of rapid economic development and technological modernization. While the original card was printed on simple card stock, of little impact on the national economy, the new card has helped to jump start a multibillion dollar domestic industry in RFID design and production.

Of the nearly \$5 billion spent on RFID globally in 2007, \$1.9 billion was spent in China, leading the market. The second generation ID project accounted for the bulk of this business, valued at \$6 billion from design to implementation. The project has stimulated China’s domestic RFID card, reader and supporting software markets such as data and system integration. Prior RFID card systems such as the social security card (deployed in more than 20 cities as of 2003,)



were more open to direct western participation, but the second generation ID project is being developed primarily by domestic firms (Batson, 2003). According to the market research firm IDTechEx, China's top 8 RFID manufacturers in 2007 were all contractors to the national ID project. The Huahong Group and its two subsidiaries provided both chip design and manufacturing, while Datang Microelectronics received government orders for chip design and chip module encapsulation. Smart card orders for Datang and Eastcom Peace helped them to a top 8 ranking among all global smart card manufacturers ("RFID in China the Biggest," 2007). Despite the government's policy to keep the ID card project among domestic firms, some foreign firms, including French Thales SA and Israeli On Tack Innovations, claim to have provided technology via joint venture (Batson, 2003).

In addition to production of the physical ID card, numerous IT firms have been contracted to develop supporting data and system integration services. Chief among them is the Shenzhen-based China Information Security Technology (NASDAQ: CPBY, formerly China Public Security Technology). CPBY has led the main pilot project in Shenzhen to test the ability to integrate once distinct information systems (health, social security, crime, education) into the national Basic Population Information Database (BPID).

The system is an integral part of the entire Shenzhen Residence Card program. Through an integrated information transfer platform, the new system will facilitate several social programs in Shenzhen, including social welfare management, one-child policy family planning management, education management and house rental management.

The system will enable various government agencies to access information regarding immigrant populations and improve public management capabilities. In the near future, the Shenzhen Residence Card Information Management System may be expanded to be compatible with other applications, such as Trans Card (an e-currency card used in Shenzhen for buses, subways and other small purchases), and could be used to access medical history, personal credit history, and driving records ("China Public Security Technology Wins Shenzhen Card System Contract," 2007, n.p..

The Pinnacle fund, the primary investor in China Public Security Technology prior to its April 2008 merger with China Information Security, tripled its stake in the company between

February and September 2007. According to a *New York Times* report, U.S. hedge funds poured more than \$150 million into Chinese surveillance companies in 2006 alone (Bradsher, 2007a).

First generation cards were so easy to forge that they spawned new forms of fraud capitalizing on the falsely placed trust of people willing to accept their proffered authenticity. Because of its comprised capacity for authentication, the national ID card was of limited value in monitoring “targeted populations” such as political dissidents and criminals. The second generation card was designed to dramatically reduce the potential for fraud and facilitate the rapid production and transfer of personal data from citizen subjects to agents of the state. The key technology affording these goals is an embedded Radio Frequency Identification (RFID) chip. The High Frequency (HF) chip could be read by a reader within a range of 20 to 30 centimeters (Lemon, 2006). According to an official of the Shenzhen public security bureau, the encryption of personal data stored on the ID card chip was so sophisticated that it could take “as much as ten million years” to decrypt (“New Card Ensures Privacy,” 2006). While one must be skeptical about such a claim, it attests to the public’s growing sensitivity to unauthorized disclosure of their personal information.

The new card dramatically reduces the likelihood of fraud while becoming the key enabler of an entirely new logic of dossier material production. Data regarding a Chinese citizen can now be automatically generated and associated with their ID with little human effort, simply with the waving of an RFID card reader. In Urumqi, the capital of Xinjiang province, police swept public streets and transportation hubs with wireless ID readers, which then linked up to the national crime database. This allowed the police not only to identify people with criminal records, but afforded the automatic creation of “mobility data” to be fed into the dossiers of all citizens whose IDs were swept (“Xinjiang Police Tightens Security Checks,” 2008).

The embedding of RFID technology affords a much higher rate of PII generation. Computer systems can be designed to generate PII simply when the card is read by a reader, eliminating the need for a human dossier administrator to produce the text on their own. If the country becomes strict about the use of the card in public places, a great deal of useful PII could be generated automatically. The public has begun to push back, however, against the strict enforcement of carrying the ID. The 2003 ID law appears far less aggressive in mandating particular uses and ties it to law in ways that the 1985 law did not.

To promote the new ID card, the Chinese government focused on the ways in which the cards would help improve the lives of Chinese citizens. First and foremost, it was emphasized that the card would help to protect individual rights. The possession of a card would ensure that a citizen could travel and get access to social services. Second, the new card would reduce identity fraud, thus reducing the impact of financial fraud on individual citizens.

Part of this public relations campaign included calling the card a “citizen card” rather than a “resident” (jumin, 居民) card. A *People’s Daily* article in the fall of 2002, announcing the planned system, explained the significance of the distinction: “While residents refer to those who live in a settled place, citizens refer to people with the nationality of a certain country who enjoy the rights as well as bear the obligations according to laws of this country” (“China Starts Working out Law,” 2002). The change in terminology also appeared to be a way of separating the national ID initiative from the increasingly controversial *hukou* system, widely viewed with disdain by the public as a state sanctioned system of segregation and exclusion. The final title for the law, however, “Law of the People’s Republic of China on the Identity Card of Residents,” retained the term resident.

The Chinese government also stressed the legal limitations on the invasiveness of the system, writing into law a list of protections against abuse. In a June 28, 2003 release via the *Xinhua* news agency, the government outlined these new restrictions:

The Resident Identification Card Law has made strict stipulations about the inspection and retention of ID cards. According to the law, with the exception of public security organs carrying out measures of residence surveillance according to the Criminal Procedure Law, “no organizations or individuals are permitted to seize resident identification cards”. If the people’s police “violate the law by inspecting and seizing resident identification cards and infringe upon citizens’ legitimate rights and interests”, they are liable to administrative sanctions based on the seriousness of the cases and if their action constitutes criminal violation of the law, they are liable to criminal investigation for legal responsibility according to the law. (“Lawmakers Hail,” 2003)

According to the new law, the second generation ID card contains the following limited information: name, sex, nationality, date of birth, permanent domicile, ID number, photograph of the citizen, the card’s issuing organ and the expiration date. This information is stored in two data formats: printed visibly on the card and stored directly on the embedded RFID chip. The key, of course, is the ID number, which allows the production and storage of dossier material on remote databases indexed by the unique number. The law refers to the ID number as the “citizens unique and life-long identity code.”

The 2003 law differs from the 1985 law in its listing of specific uses of the card. Rather than listing 17 specific uses and an open 18<sup>th</sup> category, the 2003 specifies the following four contexts in which the ID is to be used:

- (1) Changing the registered items of the permanent residence;
- (2) Military service registration;
- (3) Marriage registration and adoption registration;
- (4) Applying for handling the exit formalities;

Further, a fifth, open ended use category limits additional uses of the card to “other circumstances as provided for by the laws and administrative regulations that the citizen shall use the identity

card to prove his (her) identity.” Although this leaves the use of the national card open ended as did the 1985 law, the specific wording here appears to limit those uses to ones specifically enumerated in civil law.

#### NEXT STEP: FROM PHYSICAL TO VIRTUAL IDENTIFICATION SYSTEMS

In addition to the physical card, China is intent on developing systems to reliably keep track of citizen’s identities when they are online. Over the past three years, the Ministry of Information Industry and the Ministry of Public Security have been implementing a steady stream of “real name” policies for cell phone users, web site owners, online gamers, bulletin board users, instant messages and bloggers.

Having a universal registration system for online activity would serve at least two purposes for the dossier administrators. First, it would be the most reliable way to ensure the flow of dossier information, linking all online activity to specific, verifiable users. Second, the users, engaging in the ritual logging in process, would be reminded of ubiquitous monitoring of their activity, with the hope that they would be less likely to challenge the legitimacy of the state as they engaged in discourse with their fellow netizens. Such a system is not currently in place, however, in part because of significant resistance to “real name” policy from the public.

In mid October, 2006, officials at the MII in private meetings with members of the Internet Society of China (ISC), an industry association group, which under MII’s auspices, sets policies and standards for online business. The MII requested that the ISC study and develop a policy for the registering of real names for all bloggers. Within days of the meeting, rumors quickly began to circulate on the Internet about the impending policy, leading to a confirmation of the rumors by the *People’s Daily* on October 23<sup>rd</sup>. The article quoted the ISC secretary general Huang Chengqing: “[we] suggest, in a recent report submitted to the ministry, that a real name

system be implemented in China's blog industry." Huang also noted that much was still needed to be worked out about the policy and that this would take time. The article claimed a recent survey by the ISC showed that half of all Internet users would support such a policy.

Eight days later, one of China's most liberal newspapers, *Southern Weekend*, published a detailed account of the MII's meetings with the ISC blogging research team, suggesting that both industry leaders and the public were against such a policy in far greater numbers than the *People's Daily* article suggested.

The numbers provided by the Internet Society show that half of the netizens support a real-name blogger registration system. In the joint Internet poll conducted by New Cultural Daily and Sohu.com as of November 1, 25% supported and 75% opposed the real-name blogger registration system.

Bokee.com president Fang Xingdong was the first to introduce blogs into China. He said straight out that he is against any real-name blogger registration system. In his view, a real-name blogger registration system that violates the basic laws of the Internet will be "the biggest mistake in the history of the Internet in China"....

Fang said it is simply impossible for websites to verify the identification information of blog applicants, as it would involve huge costs of manpower and money beyond their means. (Zhao, 2006, n.p.)

In December 2006, the *People's Daily* published an opinion column from an unnamed judicial official in Jiangsu province, entitled "Bloggers should get real in virtual world." In the article, the author confirms the planned rolling out of a new "real name" policy for certain parts of the Internet including blogs and describes his support for the policy.

The authorities believe that requiring bloggers to use their real names will benefit the healthy development of Internet blogs. The free development of blogs in the past few years has led to a chaotic situation. Some have used blogs to disrupt social order and have harmed the interests of the majority. A real-name system will safeguard freedom of speech and also guarantee the sound development of blogs.

....

In fact as early as 2005 a blog-related lawsuit emerged associate professor Chen Tangfa from Nanjing University accused a blog company of having failed to properly deal with insulting comments about him that were spread by an anonymous blogger on the Internet.

Chen won his lawsuit in August in what was the first blog infringement case to come into public view. Though the court ordered the company to post a formal apology, it is hard to punish the many anonymous bloggers who wantonly vent their anger while infringing upon others' rights on the Internet. And as slander cases involving blogs emerge in an unending flow, there are increasing calls for the implementation of a real-name system.

In the virtual world of the Internet, it is a thorny issue for infringement victims to preserve evidence. The infringers attack anonymously and it is only possible to track their temporary IP addresses. So there is a clear need to develop identification technology. ("Bloggers Should Get Real," 2006, n.p.)

Negative reactions from China's net using public continued make their way into mainstream media coverage. In early January, *China Youth Daily* published a national poll of 1,843 Internet users in which 83.5 per cent were opposed to the plan. A *People's Daily* article citing the CYD survey noted that citizens were in support of a similar policy for cell phones, since they understood its role in reducing fraud and cutting down on the scourge of SMS spamming. The article concludes with a clarification of the immanent ISC policy, noting that bloggers would still be free to choose online pseudonyms, and that "real identities will remain confidential and protected if they do 'nothing illegal or harmful to the public'" ("Real-name Online Registration," 2007, n.p.).

An article published in *Liaoning Legal News* argued that the state in fact had no legal authority to compel Internet users to identify themselves and thus could not simply compel real name registration by way of ISC policy. The argument refers to the text of the 2003 ID law in which only four specific instances are listed where ID presentation is required. The 5<sup>th</sup> instance would require the passage of a national law. As a result, not only real name policies for blogs, but also those for online gaming and mobile phones have no legal basis. The article recommended that such laws be passed, noting that law abiding citizens should have nothing to fear from such laws (Martinsen, 2007).

When the government-supported industry association Internet Society of China (ISC) released its “draft self discipline code” for bloggers in May, 2007, real name registration was listed as “encouraged” rather than mandatory (Chen, 2007).

A few years earlier, however, public protest against a state anonymity reducing policy did not have as much success. On March 16, 2005, as part of the communist party’s “ideological education” campaign, China’s most popular university BBS, *ShuiMu Tsinghua*, stopped permitting access to all but actively matriculating students registered with their real names. A number of other university BBS’s across the country were similarly constrained or completely closed around this time (“China Tightens Rules,” 2005). This limited shut down of *ShuiMu Tsinghua* ended a tradition of anonymous posting and wide ranging discussion in which current students, faculty and alumni living all over the world deliberated on topics from the Iraq war to SARS to controversial issues of Chinese history.

Unlike censorship of web sites like the *BBC*, *CNN* and *Voice of America*, seen as a minor nuisance with little impact on most people’s lives, the shutdown of the SMTH and other University bulletin boards affected a large number of students and alumni and was largely viewed with great disdain. In the wake of the BBS crackdown, users reacted strongly. The access restrictions caused widespread protests, both online and, more cautiously, offline. Some Tsinghua students wrote essays and poems expressing their concern and sadness about the shutdown, while board moderators distributed ASCII BBS “posters” to relay their message of mourning and protest.<sup>38</sup> On March 18<sup>th</sup>, in a rare instance of offline protest, around a hundred students circled a monument on the Tsinghua campus engraved with the logo “actions are greater than words.” The students covered the monument with origami cranes and other paper figures, traditionally symbols of mourning. Among the more ingenious modes of online protest included the ironic use

---

<sup>38</sup> Photos of the ASCII posters and the offline protest are available at <http://maomy.motime.com/post/431462> (Accessed 3 June 2006)



of quotations by Mao Zedong to criticize the shutdown, such as “it is right to rebel!” This left BBS moderators with the dilemma of either removing otherwise legitimate quotations of Chairman Mao, or allowing the veiled criticism of the shutdown (O’Kane 2005).

Despite the outpouring of popular discontent, the policy has remained. One difference, perhaps, was that there was no BBS industry concerned about the “cost” of the plan. BBSs at universities were entirely non-profit ventures.

The Chinese public distaste for mandatory online registration slowed the process down somewhat, but it continues on many fronts. For example, a new practice in Beijing internet cafes that is likely to expand nationally is photographing and ID card scanning of every first-time customer. An October 16<sup>th</sup> *Xinhua News* article, paints a vivid picture of this new policy:

When Zhang Lihong entered Suosi Internet cafe in Xicheng District, Beijing Oct. 16, she noticed something new on the counter- a machine with a digital camera and scanner.

“Please have your photo taken, and your ID card scanned here,” the clerk stood up and said.

Zhang was confused and wanted to know why she had to do this. The clerk explained that authorities are trying to crack down on Internet misuse in the city.

The 24-year-old’s photo and a copy of her resident identity card were sent to the Municipal Law Enforcement Agency of Beijing and placed in a file.

Zhang was then given a four-digit password, escorted to a computer, and told to enter her information on an interface to activate the computer.

“You don’t need to go through the same process again when you visit Internet cafes like us,” the clerk explained. “By providing your ID number, you can check in after we verify your filed information.” (“Photo, ID Now Required...” 2008, n.p.)

The country’s lesser known IP policy, on IP addresses rather than intellectual property, also seeks to eliminate anonymity. There is strong recognition within the state bureaucracy that IPV6, the next generation Internet protocol, has the capacity to assign every individual one or more unique IP addresses so that all of an individual’s online activity can be tracked and stored. During a March 2006 visit to Paris, Hu Qiheng, chair of the Internet Society of China, told an

*International Herald Tribune* writer, “[t]here is now anonymity for criminals on the Internet in China . . . . With the China Next Generation Internet project, we will give everyone a unique identity on the Internet” (Crampton, 2006, paragraph 3). Just how significant the role of IPV6 could be in anonymity online is open to some debate. Internet policy discourse about the topic tends to point out that the protocol has considerable room for built-in anonymity, but it depends on specific implementations. Chinese ISPs could conceivably implement the protocol in ways that make it much easier to identify people via their IP addresses.

More recently, the Chinese government has been working closely with the U.N. on developing a global strategy for IP identification. The Chinese government has proposed technical standards for “IP Traceback,” a technology intended to eliminate the possibility for online anonymity via applications such as the Tor Network. A UN drafting group named Q6/17 met in Geneva in late September of 2008 to discuss the development of this system (McCullagh, 2008). As Bruce Schneier has noted, it is not clear how the UN expects to dictate global Internet policy, but the participation of the U.S. National Security Agency in the IP Traceback drafting group suggests developments here are worth following (Schneier, 2008).

## SYSTEMS OF RECORDS

The new focal site for the production of the digital *dangan* is no longer the local work unit but the Basic Population Information Database (BPID) under the administration of the Ministry of Public Security. While it is the site where much of the PII produced may ultimately wind up, the creation of the data can and does occur anywhere within the state’s boundaries; PII is produced under the administration of many of the golden projects — golden card, golden tax, golden health, golden social security, Golden Shield — but also outside state control altogether.

The Ministry of Public Security (MPS) has remained as the institutional site of one's "criminal dossier," but now maintains digital dossiers on the general population as well. The physical sites of production and some aspects of the logic, most importantly "how" the PII is produced, have been radically transformed. Two entirely new sites of PII record production have emerged as well: 1) the moment of transaction, where individual "financial identity" is constructed and 2) private companies (domestic and foreign). Both sites continue to expand in both size and importance.

This affordance of electronic networking, being able to access personal records instantaneously from great physical distances, has made possible the emergence of another entirely new dynamic of dossier record production. Data which eventually finds its way into the dossier may be originally produced within private institutions, often for entirely different purposes. In other words, these private institutions produce PII under different logics but if it has some utility to the state it may attempt to requisition the information.

To get a picture of just how state dossier record production has changed, I consider first Beijing's comprehensive informatization policies dating back to the early 1990s, and their impact on the generation and circulation of digital PII records nationwide. Then I consider record production via three major site lenses: the general population database, the construction of financial identity, and finally the "criminal" lens of the MPS. It is within this "criminal" lens that I will consider the new role of private companies as an important new institutional and physical site of dossier record production.

#### BLUEPRINT FOR MODERNIZATION

The groundwork for these major changes was laid in part by the state's comprehensive informatization policy, which began to accelerate in the early 90s. In 1992, the General Office of

the State Council developed a nation-wide office automation program, requiring all government agencies to use personal computers and electronic filing systems in their day to day operations in order to manage administrative decision making and improve public service (Seifert & Chung, 2009). In 1993, China began the first major steps toward a nationally integrated digital bureaucracy, with an ambitious plan to modernize the financial system and grease the wheels of robust economic growth.

As the opening intensified in the early 90s, this comprehensive plan to “wire” China in record time, a massive undertaking in both financial and engineering terms, became known as the Golden Projects. The Golden Projects, as originally promoted by Ministry of Electronics and Industry (MEI) chairman Hu Qili, were three in number: 1) the Golden Bridge, an ambitious expansion and modernization of telecommunications infrastructure; 2) the Golden Card, a modern financial system and central bank centered on the use of smart card debit and credit cards and 3) Golden Customs (also Gate), a plan to link the Ministry of Foreign Trade with the Ministry of Customs and facilitate state support and management of global trade. The three projects comprised the blueprint of what Ure and Liang (2000) have referred to as a “China national information infrastructure,” or CNII.

A second major goal of the informatization process was to improve government administration, in particular to make provincial and local government more transparent to central authorities. The popular phrase “the mountains are high and Beijing is far way” colorfully illustrates a historical problem Chinese central governments have had managing far flung territories. Local and provincial governments had often been reluctant to share information with the central government. Even when they did it was often false, designed to give the impression that targets were met, thus ensuring the flow of funds from the central government. Further, Beijing’s push to accelerate telecom modernization forced it to give provincial and local

governments more freedom to attract foreign investment and develop projects on their own. Although the decentralization policy was successful in stimulating ICT development, its momentum began to further threaten the central government's ability to monitor and control local government activity and opened new opportunities for corruption and graft on a large scale.

In part to counter this trend, the 1999 Government Online project called for all government departments, from central government ministries to provincial and local city governments, to connect both to the public Internet (*waiwang*) and the government Intranet system (*neiwang*). This was expected not only to improve visibility to the central government but to make local government more accountable to the citizenry.

From 1997 to 2005, the number of China government top level domains (TLDs) went from 323 to 19,800, evidence of a rapid increase in the presence of Chinese government intuitions on the public Internet. At the same time, government offices began to interconnect on the government intranet backbone as well. By the end of 2003, 97 percent of regional government agencies had established computer networks for internal usage, while 75 per cent of them had connected internal networks among their subordinate departments, bureaus, cities, and counties (Qiu & Hachigian, 2004).

Two years later, the state government launched two more projects designed to get greater Chinese society beyond state institutions wired into the national network: Enterprises Online and Households Online. Though more informal and consisting of fewer explicit targets than Government Online, the goal was to quickly get more than a million small enterprises, 10,000 medium sized enterprises, and 100 large enterprises connected to the Internet as well as for families to begin using the Internet for personal use (Zhang, 2002). Left largely to market forces for implementation, these programs have been a great success. China's e-commerce market

exceeded \$6 billion in 2007 and total Internet users as of 2008 surpassed 300 million. Online industry is booming, fueling economic growth, while opening literally hundreds of thousands of new potential sites for PII production, and a robust telecom infrastructure capable of moving these data around.

Now that we understand how the general environment for the digital production of information has changed, it is time to consider key record systems of interest: the basic population database, the financial identity database, and finally the criminal database.

#### GENERAL POPULATION DATABASE

The new focal site of production for the new digital *dangan*, the Basic Population Information Database (BPID), has been primarily under the purview of the Golden Shield project managed by the Ministry of Public security. It has also been identified as one of the four primary databases in the country's "e-government" plan, release by the State Council in 2002. "Document No. 17" outlined a common framework for the development of e-government infrastructure and applications. Using an enumeration style common in government proclamations, the document identified the key e-government initiatives as: "two networks, one portal, four databases, and 12 Golden Projects." All of these initiatives have been underway for more than a decade, but their identification and enumeration within the common rubric of "e-government" help make clear how the government itself frames the issue of ICT modernization today.

The two networks refer to a basic information infrastructure comprising an internal network (*neiwang*) for government departments and an external network (*waiwang*) connecting to private citizens and businesses. The internal network, essentially an intranet, is physically separated from the external network, the public Internet, for security considerations. Data stored in the major government databases, including PII, is exchanged between government departments

over this internal network. While major state departments develop nodes on the internal network, local governments are encouraged to develop sites in the external network, albeit with some content “logically separated” from general public access using passwords and firewalls.

The one portal initiative, perhaps the vaguest of the four, emphasizes the state government’s interest in having information for public use centrally accessible to citizens at all-in-one portal sites. As of 2004, this initiative resulted in each major government department having its own “one portal” site for general access by the public (Qiu & Hachigian, 2004).

The four databases identified in the State Council document as central to the operation of e-government are 1) the Basic Population Information Database (BPID), 2) the Basic Juridical Person Information Database (BJPID), for commercial entities and non-profit organizations 3) the Natural Resource, Space and Geography Information Database (NRSGID), and 4) the Macro Economic Information Database (MEID).

The BPID was formally initiated in October, 2002, led by the Ministry of Public Security (MPS) with the cooperation of the State Family Planning Commission, National Bureau of Statistics, Ministry of Labor and Social Security, and the State Administration of Taxation. The BPID is the largest and most comprehensive database of personally identifying information and connects to both the internal, government only network and the external, public Internet. The BPID has emerged in part via the digitization of the *hukou* system, a sub-project identified under the umbrella of the Golden Shield.

The high volume of data produced and maintained within the *hukou* system began to migrate to electronic systems in 1986. By 2002, nearly all local police stations had computerized their *hukou* system, more than one thousand cities and counties joined regional computer networks to share *hukou* data covering some 83 percent of the population, and 250 cities had

signed on to a national network for immediate *hukou* verification of close to half the population (Wang, 2004).

The digitizing of *hukou* data culminated in the completion of the BPID in 2006. The database, housed in Beijing at the National Citizen Identity Information Center (NCIIC) is said to have more than 1.3 billion entries, or one for every citizen, indexed by their unique national ID number. Although the government has not released a full accounting of the kinds of information that the database contains, it is clearly supposed to be a meta-database into which flow data from a range of other systems of records, including financial records, crime reports, education, social security and health information.

The population database operates in a tiered access mode similar to the traditional dossier system. All Chinese citizens are given at least limited access to this database, provided they have either a cell phone or web browser. Basic access allows citizens to check on the authenticity of a stranger's proffered identification. By entering the ID number and a name, the citizen can quickly determine whether the ID offered is authentic or not. If the ID and name match, the citizen is then shown a photograph for on the spot biometric identification.

#### MOMENT OF TRANSACTION AND THE FINANCIAL IDENTITY

As the primary reason for state support of informatization was economic, it follows logically that the first new site of PII production to emerge was in the financial sector (under the initial administration of the People's Bank of China). After the initial program to diffuse office automation equipment into government agencies, the Golden Card project laid the groundwork for a rapid modernization of the financial system, both standardizing and radically increasing the volume of financial data production — macro, micro and individual.



Promoting his plan to Party elite, MEI chairman Hu Qili described the Golden Card project as a way to rapidly modernize the financial system with an electronic payment and clearing infrastructure using smart debit and credit cards linked to the central bank, the People's Bank of China. Among the project's ambitious goals were 200 million debit/credit cards in use by 2000-2003 (Lan, 2004).

The Golden Card project has been hugely successful, helping to establish a booming business for smart cards (with over 80 per cent of equipment manufactured within China) and transform the country's financial system, improving supervision and management while dramatically improving efficiency. The total number of cards in use rose from 4 million in 1993 to more than 920 million in September, 2005 (Guo, 2006). Participating merchants, including stores, hotels and restaurants, increased from 20,000 to 200,000. ATMs increased from 4,700 in June 1995 to 490,000 in 2003, with card-enabled trade reaching 11.5 trillion Yuan in 2002. The bank card system has evolved into a web of interbank and inter-district information exchange networks for customer service, financial administration, marketing, risk and fraud management, and other uses (Ke, 2005). Instrumental in shifting both the public and private sectors from non-standardized, spotty, paper-based accounting to a system of detailed financial record production, the Golden Card project was soon extended with other golden projects such as golden tax, golden macro, golden finance, golden audit, and golden enterprise, to further expand the production of financial records.

As China has begun to take an interest in capital markets and the growth of its consumer economy, the need for a far more robust credit system has become apparent. Traditionally, Chinese consumers have paid for purchases with cash and do not spend beyond their means. When money is needed in the short term for emergencies, people have normally turned to members of their extended family. Banks that have loaned money to consumers for the purchase

of a car or home have done so at great risk, largely because of the unavailability of comprehensive credit histories for their customers. Banks, under the direction of the People's Bank of China, have begun to adopt the risk analysis schema of their western counterparts.

The development of a state certified "economic identity" for Chinese citizens is clearly taken seriously by the state government. The People's Bank of China (PBOC) began trial runs for a nationwide individual credit database in 2004 and officially launched the system in early 2006. At a press reception for the official launch of the individual credit database, PBOC Deputy Governor Su Ning explained the importance of the new system to the country:

A modern market economy is based on credit, where the circulation of commodities and financing are dependent on credit. In the absence of a credit culture, debts can go unrepaid, lenders are troubled by arrears, and the market is swarmed with fake and shoddy goods. As a result, huge risks face enterprises and individuals, affecting the normal functioning of the economy. Therefore, a socialist market economy has to be built on the basis of a proper social credit system.

A credit registry, as a vital part in a social credit system, provides credit information products that enable provider of credit or buyer of a financial product to assess the creditworthiness of the party who applies for a credit or the seller of a financial product for the benefit of preventing credit risks and maintaining financial stability. At the same time, by accurately recognizing corporate and personal identity and recording credit information, the system helps promote enterprises and individuals to value a good credit record. Whether a fully fledged credit registry system is available, is an important signal of whether the financial system is solidly based and market economy is maturing. A credit registry system can be regarded as the corner stone of a modern financial system and the basis of financial stability. It is of far-reaching significance for building a credit society. (Su, 2007, n.p.)

By early 2006, the database included the names of 340 million people, with roughly 10 percent of those names having credit information recorded. The database draws on a continually expanding array of information sources with all data linked to the individual's unique national ID number. In the summer of 2007, the PBOC announced that it was in talks with the State Administration of Taxation and the Supreme Court of China to track tax payments and civil compensation. In addition to regional banks, companies providing financial guarantees, telecom companies and public utilities would be allowed access to the data. The PBOC database has also

been linked with the criminal database maintained by the Ministry of Public Security. In the summer of 2008, the bank announced plans to add brokers and insurance companies.

Although the database does appear to gather information on individual credit records, there is as of yet no commercial market for this information. According to the “Provisional Rules on Management of Individual Credit Information Database,” promulgated by the PBOC on October 1, 2005, commercial banks and credit cooperatives can consult the database for the purposes of reviewing applications for credit. Other uses of the database are strictly forbidden and could accrue fines of from 10 to 30,000 Yuan. There is also very strong public sentiment against the sharing of personal data between businesses, so any change in this policy would face significant opposition. Since Chinese people still tend to prefer the use of cash over credit cards, it is not clear that transaction data would be of as much use beyond basic risk analysis. This is changing, however. China had more than 104 million credit cards in use by March, 2008, up more than 90% from the prior year (Zhang, 2008).

#### DIGITAL CRIMINALS: THE MPS GOLDEN SHIELD, AND THE TARGETED PEOPLE

The Ministry of Public Security remains an important site of production institutionally, but the physical location of data storage and the ways it is produced are also under dramatic transformation. Personal data that finds its way into the MPS dossier system today may be produced by private companies (domestic and foreign,) usually for reasons outside state national and public security goals. Further, the eyes and ears of public security are increasingly technologically augmented, with assistance from both the home grown security industry and multinationals.

As we consider the role of the MPS in the production of PII, we must remember its traditional role and the logic of the “targeted person” during the peak of the traditional dossier in

the 1980s which allowed security agents to focus their energy and manage limited resources. Although virtually all urban citizens had extensive dossiers maintained by their work units and copies of these dossiers were stored at the local PSB, only a small percentage of citizens had police agents actively producing reports about them. In part due to resource limitations, active production of a criminal file only took place for those within the targeted population.

Does the MPS still focus most of its resources on the small fraction of “targeted people?” If it does, how does the size of this population compare to traditional proportions? As we will see below, it is quite clear that the production logics of the 21<sup>st</sup> century MPS dossier system still appear to focus on a “targeted population,” but it is not yet clear how the size of this population compares to the 1980s.

In addition to digitizing the storage of standard *hukou* information, China launched its first international crime database in 2000. The database contains information for criminals previously processed throughout the country. In late 2005, the new system was credited with a steady increase in city arrest rates in Shanghai. The database’s “most wanted list” as of that year contained more than 300,000 names, 4000 of them wanted for crimes committed in Shanghai. The names of Chinese citizens coming in to register for temporary residence permit, or detained for other reasons, are run through the system to check for an existing criminal record (“Internet database tracks,” 2005).

Other, more specialized databases focus on other targeted populations, such as those in banned religious groups like *Falun Gong*. According to Hao Fengjun, a Chinese dissident who once worked for a Chinese government project to combat cults, the Tianjin branch of the “State Council Leadership Team for Preventing and Handling Cults” maintains a database containing the names of 30,000 *Falun Gong* practitioners (Einhorn, Elgin and Burrows, 2006).

Still more specialized crime databases have also been identified, such as the database of suspected drug traffickers announced by MPS Vice Minister Zhang Xinfeng in August 2005 (“China to Set up National,” 2005), and the database for people involved in pyramid-selling schemes jointly administered by the Ministry of Public Security and the State Administration of Industry and Commerce (“China to Set up Database on Pyramid Scheme,” 2006).

The logic of a “targeted population” still operates today in the process of digital criminal records production, but with some important modifications. While the eyes and ears of the public security bureau used to be men and women on the streets in the local neighborhood, the eyes and ears are now increasingly electronic, often equipment supplied by western companies in support of the Golden Shield system. Technology transfer from the west for the surveillance components of the Golden Shield project has been ongoing since at least late 2001, and has been chronicled by numerous western researchers (Walton, 2001; Gutman, 2004; Bambauer, 2006). Major contributors over the past several years include Cisco and Narus.

Cisco designed, built and sold a national system of internet surveillance, called PoliceNet, for China’s public security bureau, which is now deployed in “all but one of China’s 22 provinces” (Bambauer, 2006). Chinese telecommunications research firm ChinaNex has estimated that Cisco earns \$500 million a year from the China market and maintains 60% market share in the market for “routers, switches, and other sophisticated networking gear.” According to a report from Reporters without Borders, Cisco sold “several thousand routers at more than 16,000 Euros each for use in building the regime’s surveillance infrastructure” (“Google-Yahoo Market Battle...,” 2004, n.p.).

Another provider of advanced Internet surveillance technology to China is Narus. Consider this April 5, 2006 press release which details the company’s entry into the China

market, providing Shanghai Telecom with the capacity to identify and block “unauthorized VOIP applications.”

Narus, Inc. today announced that it has penetrated the Chinese telecommunications market with its first customer win in the region, Shanghai Telecom Co., Ltd. Through the use of the ultra high-performance NarusInsight™ IP traffic processing system, Shanghai Telecom will be able to detect and mitigate rogue VoIP traffic on their network, enhancing the quality of experience for the users of properly configured and authorized VoIP services.

In an effort to provide the highest-quality VoIP experience to its customers, Shanghai Telecom turned to NarusInsight’s ability to provide a total network view by performing deep-packet inspection (layers 2 through 7) of IP traffic, while correlating across every link of the network at extremely high speeds. This total network view is essential to the security, management and deployment of Shanghai Telecom’s IMS-based services such as VoIP, IPTV, PTT, etc. This is Narus’ first installation in China, and comes on the heels of an unprecedented agreement with the China Information Technology Security Certification Center (CNITSEC), which recently certified NarusInsight to protect China’s major telecom carriers against network attacks. (n.p.)

Although the press release here focuses on its use by Shanghai telecom in restricting unauthorized VOIP traffic, it is clear that this “IP traffic processing system” can facilitate many forms of real-time surveillance and intervention in communication networks. Among the Fortune 500 companies listed as part of Narus’s customer base is AT&T, which, interestingly enough, has been embroiled in a domestic surveillance scandal of its own, featuring another Narus product, the Narus STA, or “semantic traffic analyzer,” which was allegedly installed by NSA personnel on a major ATT network access point in San Francisco.

#### HUMAN MONITORING

To complement this technological approach to monitoring, the Chinese government employs an army of “Internet police” employed to monitor blog and bulletin board posts focused on keywords provided to them by their superiors. Many are employees of private Internet companies running bulletin board discussions or chats and not direct agents of public security. The actual number of such people doing monitoring is not easy to verify, though some estimates

have exceeded 30,000. Nevertheless, such a number would be a 1:1000 ratio of Internet monitors to users. Perhaps as a subtle recognition of their limitations, China began displaying animated cartoon police, Jing and Cha, to keep state monitoring at the forefront of online user consciousness so that they can police their own behavior.

“The Internet police has existed for a long time. This time we publish the image of Internet Police in the form of a cartoon, the purpose is to let all internet users know that the Internet is not a place beyond of law, the Internet Police will maintain order in all online behaviors,” said Director Chen of the Information Center, Internet Security and Surveillance division, of Shenzhen Public Security Bureau. (Qiang, 2006, n.p.)

In addition to monitoring real-time data streams on the Internet, the Ministry of Public Security has interest in more aggregate, processed data sets that may be stored at the facilities of private companies including email providers, search engines and social networking sites. As China has continued to open its economy, a range of international businesses have developed large-scale operations within its borders. Virtually all of these companies produce some form of PII on their customers, some of it of greater potential interest to dossier administrators. These international companies can and do make decisions that can have dramatic effect on the volume and types of PII that are created and remain available to the state over time.

#### PRIVATE COMPANIES: NEW VECTORS FOR DOSSIER PRODUCTION?

Both domestic and private companies in China today are producing PII in the course of their operations that become objects of interest of the MPS. From the available examples so far, it is reasonable to assume that the far majority of PII produced within the private sector will be released to the MPS on demand. It is critical to remember that the logics of record production within these private firms may be very different from MPS production logics, which are centered around the identification of threats. ISPs and telecom companies operating in China are required to maintain their records for sixty days to be released to the MPS on demand, but may destroy them after this time. Below are three examples to show the role that private companies are

playing: 1) the case of Shi Tao, a Chinese journalists jailed in part on PII released by Yahoo; 2) the discovery that Skype's telephone and chat service in Hong Kong was streaming personal data to MPS servers in Beijing; and 3) and the role of private mobile phone companies.

#### SHI TAO

Chinese journalist Shi Tao was arrested in December, 2004 for “illegally providing secrets to state entities.” Shi Tao was tried and convicted for sending the notes from a meeting he was attending at the *Dangdai Shangbao* (Contemporary Business News) where he worked in Changsha, Hunan Province. The meeting, held on April, 20, 2004, was called to discuss a memo from the Central Propaganda Department advising the media how to prepare for the then upcoming 15<sup>th</sup> anniversary of the June 4<sup>th</sup> pro-democracy crackdown at Tiananmen. Shi Tao and his fellow journalists were warned not to voice opinions critical of the central government and to report any suspicious meetings between journalists and democracy activists. That evening, using his Yahoo email account, Shi Tao mailed the notes of his meeting to the New York-based website *Democracy Forum*, which published them in its Internet newsletter hours later.

Shi Tao's arrest and conviction (April 27<sup>th</sup>, 2005) was based in part on evidence supplied to the Beijing State Security Bureau by Yahoo. According to the text of the criminal verdict, Yahoo account information allowed the Security Bureau to conclusively establish his identity:

Account holder information furnished by Yahoo Holdings (Hong Kong) Ltd., which confirms that for IP address 218.76.8.201 at 11:32:17 p.m. on April 20, 2004, the corresponding user information was as follows: user telephone number: 0731-4376362 located at the Contemporary Business News office in Hunan; address: 2F, Building 88, Jianxiang New Village, Kaifu District, Changsha. (“Changsha Intermediate People's Court of Hunan Province Criminal Verdict,” 2005, p. 10)

In response to widespread public criticism, Yahoo General Counsel Michael Callahan told a U.S. Congressional hearing on February 15, 2006:



The Shi Tao case raises profound and troubling questions about basic human rights. Nevertheless, it is important to lay out the facts. When Yahoo! China in Beijing was required to provide information about the user, who we later learned was Shi Tao, we had no information about the nature of the investigation. Indeed, we were unaware of the particular facts surrounding the case until the news story emerged. Law enforcement agencies in China, the United States, and elsewhere typically do not explain to information technology companies or other businesses why they demand specific information regarding certain individuals. In many cases, Yahoo! does not know the real identity of individuals for whom governments request information, as very often our users subscribe to our services without using their real names.

A year later, a copy of what was purported to be the original Beijing State Security Bureau letter appeared on the U.S.-based Chinese-language website Boxun.com. Although neither Yahoo nor the Beijing State Security Bureau have spoken to its authenticity, the Dui Hua Foundation, a highly respected human rights organization with offices in Hong Kong and San Francisco, has stated they believe the document to be authentic. Dui Hua released an English translation of the document.<sup>39</sup>

Beijing State Security Bureau

Notice of Evidence Collection

[2004] BJ State Sec. Ev. Coll. No. 02

Beijing Representative Office, Yahoo! (HK) Holdings Ltd.:

According to investigation, your office is in possession of the following items relating to a case of suspecting illegal provision of state secrets to foreign entities that is currently under investigation by our bureau. In accordance with Article 45 of the Criminal Procedure Law of the PRC, [these items] may be collected. The items for collection are:

Email account registration information for huoyan1989@yahoo.com.cn, all login times, corresponding IP addresses, and relevant email content from February 22, 2004 to present.

Beijing State Security Bureau (seal) April 22, 2004

Assuming the document is authentic, it challenges the Yahoo general counsel's claim that Yahoo "had no information about the nature of the investigation." Shi Tao was sentenced to 10 years in prison.

---

<sup>39</sup> Retrieved February 5, 2008 from [http://www.duihua.org/press/news/070725\\_ShiTao.pdf](http://www.duihua.org/press/news/070725_ShiTao.pdf).

## SKYPE AND TOM.COM: LOGGING USER CHAT TRANSCRIPTS

Activists at the University of Toronto's Citizen Lab discovered a cluster of eight message-logging computers operated by the HK company Tom.com as part of its joint venture with Ebay's Skype service. Tom.com has been distributing Skype IP-telephony and chat software for use in mainland China. Although it has come to light previously that Skype and other Internet services in China were abiding by local regulations and censoring sensitive content, Tom's practice was taking this a step further and actually logging text conversations containing certain trigger words. These words included standard black-listed phrases like "Free Tibet" and "*Falun gong*," but also the terms "earthquake" and "milk power," referring to the fall 2008 scandal of tainted baby milk.

What made this case so problematic was that Skype had explicitly stated before that, although it did censor taboo chats, communications data was simply disregarded and not retained. Instead, the University of Toronto researchers discovered that anytime a sensitive keyword appeared in a chat the entirety of the text was stored on one of these servers along with personally identifying information of the chat participants, such as their IP addresses and their Skype IDs. This information was being retained not only for Chinese citizens using the Tom-Skype software to engage in chat, but also any foreign counterparts they might be chatting with. The computers were also storing calling records for Skype voice conversations containing names and in some cases phone numbers of the calling parties. According to the researchers, these 8 servers had archived more than 166,000 censored messages from 44,000 users in just two months (Villeneuve, 2008).

As Internet furor both inside and outside China grew, the CEO of Skype issued a carefully worded statement, apologizing and announcing that the practice would cease.

Acknowledging that the trust of Internet users had been put at risk, the CEO said that their joint venture partner, Tom.com, had been engaging in the practice without their knowledge.

#### MOBILE PHONE TRACKING AND SEARCH DATA

Chinese domestic ICT companies likely provide information to the Chinese government upon demand, as they have no legal authority to resist and are unlikely to suffer any public relations damage if the news were to get out. The average Chinese citizen simply expects that the government gets access to its personal data.

The head of China's biggest mobile phone company, which has more than 300 million subscribers, stunned delegates by revealing that the company had unlimited access to the personal data of its customers and handed it over to Chinese security officials when demanded.....

"We know who you are, but also where you are," said the CEO of China Mobile Communications Corporation, Wang Jianzhou, whose company adds six million new customers to its network each month and is already the biggest mobile group in the world by users.

He was explaining how the company could use the personal data of its customers to sell advertising and services to them based on knowledge of where they were and what they were doing.

When pressed about the privacy and security implications of this, he added: "We can access the information and see where someone is, but we never give this information away ... only if the security authorities ask for it." (Plowright, 2008, n.p.)

What Chinese citizens and consumers are more likely to complain about is the sharing of this kind of information with other private companies. Nevertheless, this general sentiment has not kept the lid on the emergence of a nascent market for personal information commodities. Consider this 2006 press release by the mInfo company, based in Shanghai.

Data published by mInfo are based on actual usage information over the last year across its SMS, WAP, kJava and IM mobile search systems. mInfo is the only provider in China offering search over all four models enabling nearly all mobile users in China to access its service. This gives it a much broader view on what users are looking for versus most other vendors that only provide WAP-based search....

In general, mobile searchers are looking for answers surrounding their daily lives. mInfo's data shows that searches were spread fairly evenly amongst the basic subject areas of Local Search (41%), Informational Search (31%) and Rich Content Search (28%). Local search involves finding directory information for locations such as bars, hotels and ATMs. Informational search relates to finding things such as stock quotes, sports scores, price promotions and flight schedules. Rich content search relates to finding ring tones, pictures, mp3, games, etc. mInfo offers over 30 search categories within these three areas. Mobile search traffic seems to pick up each day around noon and ramps steadily until about 10pm when traffic peaks. Fridays and Saturdays are the most heavily trafficked days for mobile search services. ("What were China's 450 million," 2007, n.p.)

## CONCLUSION

While China's recent history includes a period in which much of the urban population experienced a highly effective and oppressive state dossier system, the primary means by which dossier materials are produced have been in a process of rapid change. As this period of transition is still ongoing, it is difficult to say yet how China's digital dossier system will ultimately compare to the capacity of the traditional system. While new technologies afford unprecedented volumes of PII production and aggregation, the public has a growing fondness for anonymity and privacy.

Even given a near total capacity of the Chinese state to requisition PII on demand, data cannot be requisitioned if it is not first produced. Chinese companies have only begun keep digital records within the past decade and still lag behind U.S. companies in volume and detail of PII production. China is catching up rapidly, however. The Internet market is booming and the new businesses springing up there have become quite adept at gathering, storing and manipulating personal information.

So far, there remain spaces of anonymity within the Chinese electronic networking systems and in public as well as a strong and perhaps growing public voice in support of it. Chinese citizens as a group have succeeded in limiting the required uses of their national ID

cards. They have maintained the right to blog online with the presumption of anonymity. Although we can begin to call this presumption into question (especially with the diffusion of IPV6 ) there remains an active public interest in it that will continue to develop, one that could establish a legitimate discursive identity within China's project of modernization. Although it is certainly too early to tell, there are major positive signs that should not be ignored.

## CHAPTER 7: SYNTHESIS

Few would challenge the proposition that China maintains a state dossier system or that this system facilitates an oppressive interface between the state and the public. Countless academic and popular press articles refer to China's surveillance systems in Orwellian terms. That the U.S. and China come from two entirely different political traditions is indisputable, but these case studies have shown that the practical differences today, when it comes to the ongoing evolution of state dossier systems and the specific constraints they encounter, are not as significant as we might assume. Now that I have reviewed the two cases on their own terms, I will juxtapose them more directly here in four sections: *The Four Drivers Compared* revisits the four drivers of dossier systems outlined in chapter two (technology, political economy, law and public sentiment); *Towards a Vocabulary of State Dossier Systems* explores in more detail the linguistic toolkit that has been developed for state dossier system analysis, including terms like the *sites and logics of production* and the *targeted person*; the *Defense of Claims* section reviews some of the more potentially controversial propositions that have been presented here and the evidence on which they are based; finally, the chapter offers *Concluding Thoughts*.

### THE FOUR DRIVERS COMPARED

#### TECHNOLOGY

Both the United States and China rely on advanced technologies from western corporations like Cisco, Nortel and Narus. While the West is a major source of advanced surveillance technologies ranging from hardware to software, China produces most of the CCTV cameras that are deployed in the U.S., including the newest generation of wireless IP cameras that can be more easily accessed by centralized, state, local and federal policing institutions. In recent

years, a new phase of home grown surveillance technology development is occurring in China with investment from western financial firms.

Today, one can argue that the Chinese second generation ID card technology affords a much greater range of dossier production possibilities than does the 2D bar code on the U.S. Real ID. While the Chinese card can be read from a distance in any direction (360 degrees) from the card, the Real ID card requires a direct line of sight. Given this basic comparison, it is clear that the number of real world situations in which a state agent could identify and generate or retrieve data on a target individual would be much greater than comparative scenarios with the 2D bar code.

It is important not to overstate the significance of RFID as a driver of dossier production. There are a range of other devices diffused through the global social system that afford ubiquitous ID and location for those who carry them, such as cell phones and GPS devices. The user has the option of not carrying a particular device. He can leave his cell phone behind, or temporarily remove the battery. He can buy a used car that does not carry the built in GPS device, or choose to queue up in the slow non-EZPASS lane at the toll booth. He might choose to leave the ID at home as well, but the viability of that option will depend in part on the governing legal and policy regime. It is not difficult to imagine a future in the U.S. in which one would need to present state ID to board any form of public transportation. In such an environment, the choice to leave one's ID at home might come at the expense of mobility. A card that must be presented to board public transportation or when making use of public thoroughfares is likely to have a significantly higher effective coverage than any of these other devices.

Although the majority of adults today carry cell phones whenever they are out in public, availability of this identifying information is much more limited. Only the person's cell service

provider has ready data access. Other private businesses do not generally have access and even state and federal law enforcement are subject to legal access restrictions of the ECPA. Nothing in the final rules proposed for Real ID limit private commercial access to basic identifying information stored within the MRZ (machine readable zone). Given federal court approaches to reasonable expectations of privacy in public, it is highly unlikely that citizens will benefit from constitutional protections over the collection of a person's location information broadcasted by their ID card. Under the current legal and policy regime, the constraints on taking advantage of the indexical identifying information presented by the RFID embedded ID card are far less significant than those for other devices. It will be up to the legislative branch to provide statutory protection to return some balance, and give back legal boundary negotiation resources to the public.

One could argue that RFID's are really only generating PII at the point of transaction, increasing the speed and efficiency, but not necessarily the volume, of personal data production. Taking heed of Marx's "surveillance slack," we must not assume that simply because it is technologically possible to produce PII in circumstances where it was once not possible (or at least resource intensive) it means that this data will be produced. This is an important point, but it is also important to recognize the degree to which former constraints on data production have been eliminated and the potential for actors in both public and private agencies to see enough value in this information to take advantage of these affordances. In addition to the ID card itself, the average person will be carrying a growing number of other tagged objects — clothing, credit cards, money, media — that help narrate their personal story, facilitating profiles for risk and reward. While the objects individually may still bear some traces of anonymity (depending in part how commercial RFID legislation evolves,) the card would act as a continual indexical identifier, increasing the value of the information beyond its immediate commercial context.



As was discussed in chapter 4, however, while the Real ID program appears to be on its last legs, other federally supported ID technologies are waiting in the wings to take its place. Both the U.S. Passport Card and the Enhanced Driver's License contain proximity RFID chips with read ranges exceeding 30 feet, much greater than the 20 to 30 centimeter read range of the chips embedded in China's ID card. Despite organized public resistance in opposition to the deployment of RFID within human identity systems, it appears that the U.S. government is determined to roll out these cards in greater and greater numbers.

Although it was fashionable early on to speak of fax machines, cell phones and the Internet as "Technologies of Freedom," as time has passed it has now become equally fashionable to frame new communication technologies as powerful tools of state surveillance. As was noted in Chapter 6, there has been some cooperation between the U.S. and China in a UN committee to decrease or eliminate anonymity online via the embedding of new technologies into the TCP/IP protocol. The IP Traceback initiative overseen by the secretive Q6/17 committee appears to be looking for ways to prevent such things as anonymous blog posting via proxy server with the implementation of new technology.

Technologies of resistance designed in the U.S. such as the Tor project, client-server software that facilitates anonymous Internet browsing, are widely used in China. Software tools to generate fake online IDs have been developed and widely used in China to circumvent requirements for online gaming, but the pace of both raw technological development and international standards appears to favor state monitoring over individual and collective resistance. This is, of course, a difficult future to predict. I will, however, consider some general projections of technological development and their impact on potential configurations of state dossier systems in the coming decades.

There is no doubt that advances in ICTs have dramatically increased the possibilities for the state to aggregate and process information, but these advances have not and never will lead to unlimited information processing capacity. Today, both public and private institutions are motivated to store any and all information they come across if it may have potential value sometime in the future. The cost of data storage continues to drop at rates faster than Moore's law so, ignoring the privacy implications, this default storage policy appears to be very sound logic given the current and likely future state of the technology.

According to research conducted by the IDC, however, this picture is in the process of changing, not because the advancement of storage technologies is expected to slow down, but because the overall rate of information production is expected to exceed this rate. As of 2007, according to IDC estimates, all of the empty, available data storage media (primarily disk drives, tapes and optical storage) totaled

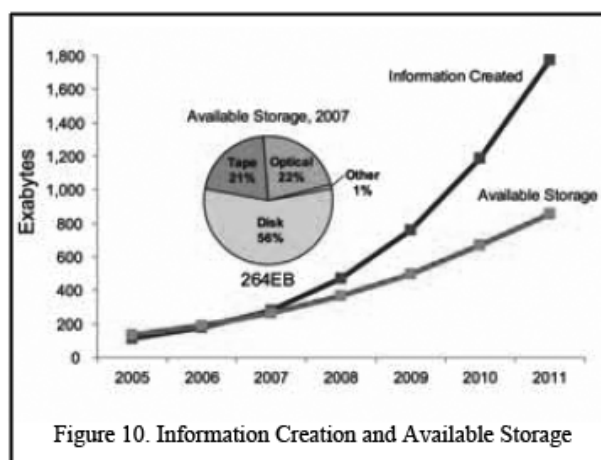


Figure 10. Information Creation and Available Storage

approximately 264 exabytes, approximately equal to the total volume of information produced in that year. Since most of the information produced in a given year (despite the increasing trend for businesses to save their data,) is what is known as transient data and is either overwritten or disappears into the ether, modern society experiences no shortage of storage capacity today. As this gap widens, however, it “will put pressure on those responsible for developing strategies for storing, retaining, and purging information on a regular basis” (Gantz et al, 2008, p. 4).

Another related question connected to technological affordance is the relation between data volume and capacity for analysis. Prior to the age of data mining, any file or record of

information would need to be processed by a human being. Increases in the volume of this data could quickly overwhelm human cognitive capacity and subsequently impair their ability to produce accurate, actionable intelligence. With the advent of data mining, however, the picture appears to become cloudier. The capacity for computers to process and analyze large data sets, while not infinite, far exceeds human capability and thus appears to change the balance. The Total Information Awareness program was based on the assumption that sophisticated software programs could churn through the totality of available data and divine patterns of terrorist machinations that would enable state authorities to apprehend the terrorists before they struck. If data storage were to become a noticeably scarce resource for government and industry, this could put pressure on innovations in processing algorithms or impact the evolving logic of dossier production. It is difficult to predict with any confidence how this dynamic socio-technological process will turn out.

#### POLITICAL ECONOMY

The political economy of the U.S. and China, in general terms, are much more similar today than they were in the 70s and 80s. Today, large, privately owned corporations in both countries compete for the same sources of capital, bid to overlapping pools of customers, and conduct their business within an increasingly international set of trade regulations and law. Surveillance is being at least partially driven in both countries by market logic. According to the Washington-based market research firm Homeland Security Research Corporation (HSRC), the U.S. Homeland Security (HLS) industry is projected to grow at an average annual rate of 50%, reaching \$34.8 billion by 2010 “assuming no new major terror attack.” In China, one estimate projects that its market surveillance hardware and services will be in excess of U.S. \$43 billion by 2010 (Meyerson, 2007). Many of the multinational corporations which are benefiting from the emerging surveillance industry, such as Cisco, IBM, Nortel, and Narus are operating in both

countries. A significant portion of financing for the leading Chinese surveillance companies is coming from U.S. investment firms. China Security and Surveillance Technologies (CSST), for example, which listed on the New York Stock Exchange on October 31, 2007, received more than \$110 million in convertible loans from the Chicago-based hedge fund, Citadel Group (Meyerson, 2007).

As the U.S. state dossier system is a hybrid of public and private institutions, any restrictions on private activity related to dossier systems is likely to have a constraining effect on the system as a whole. Historically, however, the federal government has refrained from regulating related private activity. Although the HEW committee in 1972 recommended prohibiting the use of SSNs in private business activity, the final form of the Privacy Act contained no such provisions. With a similar policy opportunity arising with the U.S. Real ID program, the federal government again refrained from regulating its use in private business. In China, the 2003 National ID Card law formally prohibits non-state entities from seizing a citizen's ID card and narrowly restricts the basis upon which even state agents such as police may demand the card. While China's legislature continues to moot its own privacy law, the lack of a free market tradition makes it more likely that restrictions on the commercial exchange of private information could be put in place. Given the growing role of law in the business world, it remains likely that such a law would be enforced. Restrictions on the collection and exchange of personal financial information other than for purposes of reviewing a credit application have prevented the emergence of a commercial market for such information. The Chinese public also remains strongly opposed to the private exchange of this information.

The interest of private corporations in surveillance infrastructure goes beyond its own profitability and extends to its function in helping to protect control over intellectual property.

The International Federation for the Phonographic Industry (IFPI), for example, issued a report in 2007 which argues for aggressive surveillance worldwide, including in China:

As an industry, we enforce our rights decisively, and this will continue. In 2006, we had significant legal victories, led by a U.S.\$115 million settlement against Kazaa. We were told we could never track down such offenders on the internet. We were told they would hide in places where we could not find them! (“IFPI:07 Digital Music Report,” 2007, p. 3)

At one time you were considered a new media philistine if you wanted to regulate the internet. But then Google promised the Chinese government that censorship was possible. Then Google blacklisted BMW in the internet world for anti-social behaviour. It seems policing is acceptable for all sorts of things but not intellectual property! (p.3)

Whether China does succeed in harnessing digital channels for a new vibrant legitimate music market very much depends on how seriously a commitment the country and its key operators will make to protecting and enforcing intellectual property rights. The recording industry supports the U.S. Government’s moves to raise the pressure on China, if necessary via the WTO, to ensure effective enforcement of intellectual property rights. (p. 7)

## LAW

It is important to recognize the issues involved when attempting to compare two highly contrasting countries on the dimension of law. We do not have any reason to assume the authority of the law is the same in each country. At the same time, a law is a particular kind of document that represents a formal production of the governor of a social system. It is the product of tensions between the state and its people and among classes and sectors of the population, regardless of whether or not these tensions are mediated in a formal democratic system. One can make inferences from that document about these tensions and often identify a range of stakeholders.

It is clear if one studies recent Chinese history that citizens are not as pliable *vis a vis* the state regarding identity systems as they once were, and they have gained new interests in their informational privacy *vis a vis* the commercial businesses they interact with on a daily basis. The 2003 National ID law enumerates a much smaller set of circumstances in which citizens must present their ID than the 1984 law. The far majority of Chinese citizens do not feel pressure to

carry their ID cards despite the law. Law targeted at the commercial sector is growing rapidly along with enforcement mechanisms. Although admittedly difficult to make a direct comparison, private firms doing business in China must increasingly come to terms with statutory regulations.

The role of private companies in the production of records for the dossier system is critical in both the U.S. and China. Constraints on commercial practice can significantly limit the potential of the state to assemble dossiers, since it would reduce the scope of extant (produced) PII. Given the U.S.'s modern legal history (some of it described in chapter 3,) it appears highly unlikely that the U.S. would ever significantly constrain the private sector in its production and retention of PII. The Chinese public, already sensitive to abuses of personal information by private companies, is exerting some pressure for more accountability. The legislature is more likely to respond in the China case, as "free market" and other liberal democratic discourses have less traction.

Although it certainly exists within a tradition of the rule of law that China clearly lacks, the U.S. legal system is experiencing its own period of transition and internal contradiction as it adjusts to both the rapidly changing technological environment and the increased concern for security subsequent to the September 11<sup>th</sup> attacks. Due to the bright line distinction between information in storage and that in transmission and the comparatively weak protection of information privacy in stored data, the U.S. federal government has many legal options open to it for the collection and aggregation of personal information. A long standing policy to avoid interfering with the personal information practices of private businesses coupled with a growing reliance of the state on these same private institutions for the bulk of its intelligence activity (Shorrock, 2008) means that a shrinking and increasingly insignificant percentage of U.S. personal information practices falls under the purview of either the Privacy Act or the Fourth Amendment. As we understand more about the manner in which state dossier systems are

produced, we begin to understand that the U.S. legal system does not constrain its development in any significant way. Though some restrictions on real time state surveillance remain, the state's ability to get personal information from the private sector, both voluntarily and via force of administrative subpoena (NSLs), has few practical limits.

Further, the growing practice of watch lists allows the government to not only collect a wide range of PII on non-criminal U.S. persons but to act on this information entirely outside of judicial review. The process by which citizens are nominated for inclusion on a particular list is kept secret for national security reasons, while the agency that subsequently acts on such a listing, inconveniencing, detaining, or otherwise physically interfering with the lives of the listed subjects, is not deemed legally responsible for acts based on incorrect information.

While one might argue that the law in China has no true authority over the state in the way that the Constitution has over the U.S. government, this dissertation has established that the Constitution does not place any significant constraints on dossier practices. Dossier practices within fusion centers, for example, lie almost exclusively outside the jurisdiction of federal laws and policy. At the same time, we must be careful not to understate the significance of notice requirements in the Privacy Act. While it is indeed true that agencies may choose not to give notice by assuming an exception for their particular record system, details that have emerged in SORNs and PIAs made the research in this dissertation possible

A dangerous trend, however, has been emerging. There appears now to be a growing assumption within the executive branch that it can selectively ignore aspects of the law that it believes interfere with the prosecution of the War on Terror. A recent book by Jack Goldsmith (2007), the *Terror Presidency*, provides a first-hand account of disregard for law in the Bush Administration in the context of the national surveillance program. The Bush administration

tested and in fact exceeded constitutional and statutory limits on real-time surveillance. The adoption of signing statements has dramatically reduced the effective resolution of congressional law and the courts seem to be deferring to executive will on these matters (Sewell, 2006). A report by the American Bar Association (ABA) in 2006 noted that the Bush administration's use of signing statements during bill signings was "contrary to the rule of law and our constitutional system of separation of powers" ("The President v Congress," p. 5).

Although it would be tempting to label this selective contempt for the rule of law as a particular excess of the Bush administration that will not be repeated, one could argue that this approach is a characteristic of the post-9/11 U.S. state that is persisting into subsequent presidential administrations. Despite an explicit campaign promise to stop the practice of signing statements, Obama, as of June 2009, had issued more signing statements than had Bush at the same time in his presidency (4 to 1). Human rights activists have already criticized the Obama administration for its position on administrative detention and warrantless wiretaps, arguing that in many ways the Obama administration's position is even more extreme (Greenwald, 2009; Jones, 2009).

#### PUBLIC SENTIMENT

Despite the strong tradition of privacy in Western culture and in U.S. legal history, its ranking compared to other social values, namely security, has changed dramatically since the September 11<sup>th</sup> Terrorist Attacks. Young Americans appear to value privacy less in the context of interpersonal relations, but they actually value privacy more than older Americans in the context of government surveillance (Berton, 2006). Although privacy has not been as important a cultural value in China as in the West, there has been a nascent privacy movement in recent years (Lu, 2005), culminating in the state's relenting to public pressure to abandon its Real Name project and to preserve, at least officially, anonymity in blogging for Chinese citizens (Dickie, 2007).



Public sentiment can have a major effect on public policy no matter what the political system. Before public sentiment can play this role, however, the public must be educated and aware of the problem at hand. The public must understand why state dossier systems are a threat to the public interest and what characteristics of a state's orientation to the personal information of its citizens are problematic. Chinese under the age of 40 today live with the memory of China's totalitarian oppression and have a particular appreciation for the freedoms in today's modern society that many Americans take for granted. In the U.S., polls have shown that support for privacy is greatest when asked about in the abstract (Best, Krueger and Ladewig, 2006). Support for privacy in general remained relatively stable from 1997 through 2003, actually rising by a few percentage points immediately after the 2001 attacks. In 1997, 78 percent of the population agreed that it was "essential that they have the right to privacy" (p. 376). Yet while support for privacy remains high in the abstract, it drops when the questions become more specific or when the privacy right is juxtaposed to other interests like the fight against terrorism. In June 2002, a comparable percentage of Americans (79 per cent) agreed that it "was more important to investigate terrorist threats than to avoid intrusions on personal privacy" (p. 378). While this number dropped the following year, it was still 73 per cent. In May, 2006, the *Washington Post* asked respondents a similar question, and found that 65 per cent of Americans felt federal government investigation of terrorist threats outweighed any accompanying intrusions of personal privacy ("Washington Post-ABC News Poll," 2006).

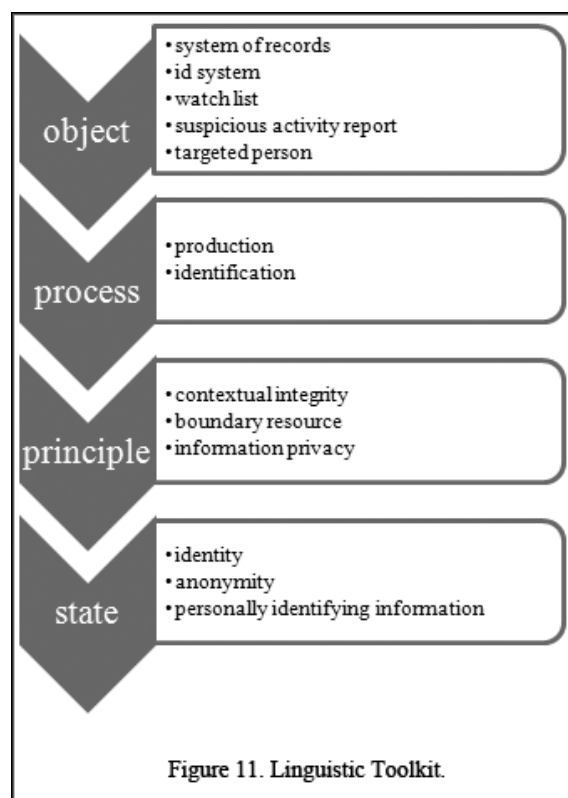
It is interesting to note some common aspects of successful public efforts to limit or hold back the advancement of the state dossier system. In China, student opposition to the Real Name system for university bulletin board systems, despite its creativity, was not able to turn back state policy. It was not until Real Name opposition expanded to include the commercial Internet sector, which, beyond any moral arguments, saw the requirements as likely to accrue large and

unnecessary costs, that resistance became strong enough. Similarly, in the U.S., the “success” of Real ID opposition would likely have had a much different result if states had not been concerned about the federal imposition of an “unfunded mandate.”

Without considering the specifics of the political systems in each country, one can say that the idea of democracy is that institutions are in place that can successfully translate the will of the people into the active machinery of government. Authoritarian or totalitarian governments, on the other hand, often operate in direct opposition to or ignorance of the people’s will. In countless situations, in plans to put RFID in identity documents, in travel systems which categorize travelers according to their terrorism risk, in tips systems which invoke the public and certain private sector positions to report suspicious activity of their fellow Americans, we see a repeated pattern in which the U.S. government pushes through policy, pushes through particular components of the state dossier system, despite acute public opposition. In most situations, this is accomplished via a change in name rather than substance. We get ATS Instead of CAPPs, the ISE instead of TIPS, Guardian instead of TALON. But in other situations, the desired state policy, such as the use of proximity RFID tags in identity documents, is simply rammed through despite overwhelming public resistance.

## TOWARDS A VOCABULARY OF STATE DOSSIER SYSTEMS

In the first chapter of this dissertation I discussed the importance of language and framing in the problematization of particular surveillance practices. Over the course of research and writing, I have developed a set of terms and phrases, a “toolkit” for the discursive problematization of state dossier systems, terms that can be used across individual state dossier systems. Some of the most significant terms used in the problematization, terms that can be abstracted from particular case contexts and used as part of a general model of the state dossier system, include: *system of records*, *ID system*, *production*, *targeted person*, *boundary resource* and *identity*. Many of these terms are existing terms of art, while some have emerged from the research process. For example, I leverage the terms “contextual integrity” and “boundary resource” without attempting to alter or expand their definitions in any way. For the much more general, but even more

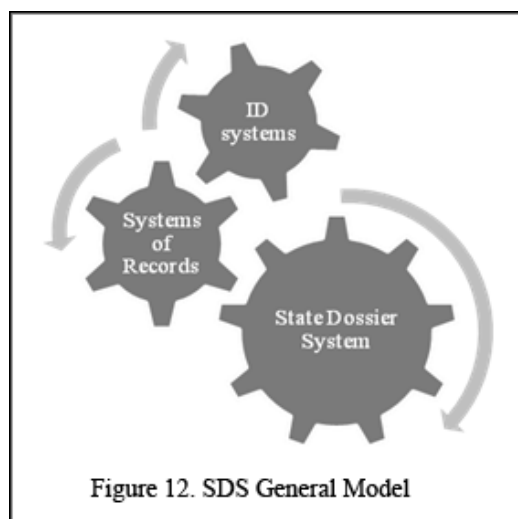


critical term “privacy,” I explored the dynamics and demonstrated the cross-cultural value of the concept in great detail in chapter 5. In other cases, such as the term “personally identifiable information” and its variants, I attempt to draw the term in sharper relief than has commonly been the case.<sup>40</sup> Still other terms, like production, and the “sites and logic of production,” represent

<sup>40</sup> I have contributed what I hope is a set of more precise terms to illuminate often overlooked distinctions and help clarify the degree of anonymity or identification associated with a given record. I will not repeat that discussion here; it's on page 13, chapter 2.

what I hope is a new and useful way of linguistically modeling state run dossier system. The phrases “targeted person” and “person of interest” are local, case-based phrases that represent a common aspect of all state dossier systems: the categorization of particular subsets of people for heightened scrutiny. This is what Lyon (2002) calls “categorical suspicion” and manifests in the watch list.

In any model, the interrelationships between model components are critical and the state dossier system is no exception. One must be careful here, because it is easy to mistake a particular architecture within a system for a general rule. These terms can be clustered in different ways depending on the semantic rules we approach them with. In the illustration (figure 11), I group the terms according to the following categories: object, process, principle, and state. Objects tended to become case nodes, while processes, principles and states play a significant role in analysis. There are different ways these terms might cluster and otherwise interact with one another. I begin with one very basic relationship which I do claim is a general rule of state dossier systems: that between the ID system and the system of records.



**Figure 12. SDS General Model**

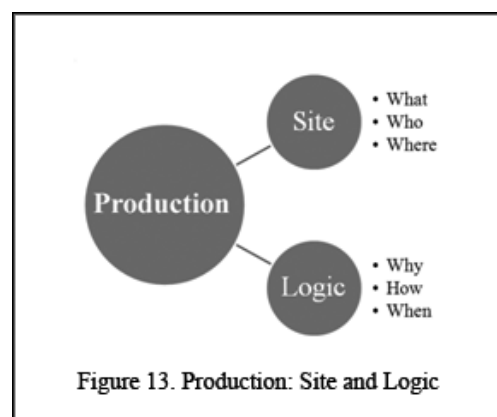
While this distinction is important, it is critical to remember that it can be expressed in many different information architectures. There might be one ID system and one system of records that functions as a state’s dossier system (as one might simplistically model the current Chinese system) or it might consist of multiple, interconnecting systems of records leveraging a range of ID systems with varying scope and reliability. Further, the distinction is not mutually exclusive; ID systems can only function when linked to a system of records that holds the

associated identities. The Commercial Driver's License Information System (CDLIS), for example, is the basis for authentication of commercial driver's licenses nationwide. Nevertheless, many, many distinct systems of records containing personal information are designed, produced and maintained without the designers needing to pay attention to ID systems at all, as they piggy back on an existing system such as the driver's license or social security number.

Production is an important term, perhaps the most distinctive term within this linguistic tool kit. The records within these systems do not simply exist out there. They are always first produced, and produced according to specific logics and specific sites of production that shape the quality and ultimate effect that the records have on the interface between the state and its people. Although the terms "watch list" and "suspicious activity report" were used exclusively within the U.S. case, they are clearly applicable to the China case as well.

## PRODUCTION

China's dossier system is currently undergoing a major transition from the production of single, localized paper files to an at once highly distributed and highly centralized system of electronic records and identity cards. During this transition, both the sites and logics of personal information production are in the process of dramatic change, opening up new possibilities for resistance in the process. In the United States, a new class of PII, PII of suspicion, is being produced on state authority at an accelerating rate. The Suspicious Activity Reporting (SAR) system leads to the production of PII that are woven into the state's counterterrorism



narrative. Innocent people on the street engaging in First Amendment activities or simply minding their own business may be “interpellated” (Poster, 1996) into a government counter-terrorism database within a narrative of suspicion and threat.

The entailments associated with the use of the term production (instead of the more passive “collection” or “gathering”) are highlighted with the accompanying terms “site” and “logic” of production. These terms allow us to focus on the specific institutional and social settings in which particular kinds of personal information are produced, while highlighting points of leverage for law and policy. Below I offer some general impressions about the sites and logics of personal information production that are applicable to the research and analysis of any state dossier system.

## SITE ANALYSIS

### WHAT?

What is the specific content of the record and in what medium is the record embodied? At the site of production, personal information is not simply being captured or collected but a specific form of record is being produced. The record has precise semantic content that plays roles in discursive formations that sustain communities of meaning and action from the small group to the institutional level. The specific physical manifestation of the record — as a manila folder of 10 white cotton pages or as an electromagnetic disturbance on the surface of a hard disk — places specific constraints on the extent and scope of the dossier systems it might populate. These details have tremendous impact on how this information subsequently circulates, how it is associated with other information, how it is used and what impact it has on its subject.

## WHO?

Although the subject of the personal information within a particular dossier system record is clear (it is indexed to the subject), the record itself may have been directly produced by the subject, it may have been produced by someone intimately involved with them, it may have been produced by a third party who had little or no regular association with the subject, and it may even have been produced by a machine. Clearly, who (or what) produces the record has a great deal to do with the particular qualities of the record and the relative influence the subject has over its production.

## WHERE?

The answer to the where question of dossier record production could be either physical, institutional or lexical-semantic.

## PHYSICAL

This question of physical storage is complex. The site at which personal information is produced may not be the same location where it is ultimately stored. A surveillance detection report (SDR) produced by a Federal Marshall patrolling an airport waiting lounge may only be temporarily stored in his or her handheld device before it takes more permanent form in the federal TISS database.

A record, for it to be observed, must manifest via some physical substrate, even when the medium is electronic. Ultimately, a record is stored on at least one specific, physical server. The location of the server is often more than a curiosity as it may determine the particular laws or regulations it may be subject to. This is important not only at the national level but also within national borders. Data stored locally within a particular U.S. state, for example, may be under different legal requirements than that stored on a federally owned server in Washington, D.C. The

Information Sharing Environment, especially the notion of shared spaces, operates this way, making locally maintained, locally regulated data accessible to the federal government while it remains outside the domain of what are usually stricter federal laws and policies.

#### INSTITUTIONAL

Understanding the institutional location of personal information production tells us not only the organization responsible for the record, but also much about the role this information is intended to play.

#### LEXICAL-SEMANTIC

Though the lexical-semantic location may seem too abstract and theoretical, it is actually of considerable importance. When someone is searching for information today, more important than the information's physical or institutional location is its position within textual space, navigable via three overlapping topologies: semantic, lexical, and link. Records may be associated by shared meaning (searching Google for information on restaurants in Philadelphia,) by the presence of a specific lexical identifier such as a unique identity number, or via a hypertext link.

#### LOGIC ANALYSIS

##### WHY

What is the motivation for a particular moment of production? Why is the producer making the effort to produce such a record of personal information in the first place? Are they logical reasons or are they based on faulty reasoning? I identify four key factors that drive these moments of production: *use value*, *exchange value*, *legal or policy requirement*, and *technological affordance*.



### USE VALUE

When the state is publicly selling a new initiative, use value justifications are usually at the forefront. Use value means that the producer is storing the subject's personal information based on the belief that it will serve some direct use in the provision of service to that subject or to a collective for whom these individual behaviors are relevant. The data might add to some general understanding about human nature, for example, that allows a company to better navigate and capitalize on its targeted market. For a government agency, use value might mean that storing the information would allow it to make better decisions about distributing limited resources, or identify potentially dangerous individuals who are a threat to the public welfare or national security.

### EXCHANGE VALUE

Exchange value means the agent is producing the information based on the belief that they will be able to sell it on the open market for cash, or to trade it for some other benefit. The growing market for data mining companies in the U.S. drives companies in many different sectors to produce information on their customers that they may not otherwise need, that may not have direct use value within the context of their business.

Companies within the financial sector, from banks to casinos and gold dealers, may produce suspicious activity reports for their "negative exchange value," meaning that they produce SARs out of the knowledge that not producing them could cost them significant amounts of money. Wanting to avoid financial liability for non filing and protect themselves from liability for unnecessarily filing reports, banks increasingly err on the side of "caution," filing whenever customer activity has the slightest tinge of suspicious behavior.

#### LEGAL OR POLICY REQUIREMENTS

This category covers a wide range, from explicit legal requirements to policies established by particular agencies for the production and retention of data. U.S. banks, for example, are required by law to generate reports of all transactions exceeding \$10,000 in value and any transactions over \$5,000 deemed suspicious. Local police are given policy guidelines that identify particular situations in which the production of a SAR report is warranted. The Chinese government requires that all ISPs within the country record and store activity logs for its customer base for at least 90 days.

#### TECHNOLOGICAL AFFORDANCE

Technological affordance means that some technological device in use by the agent is configured in such a way that the data is stored as a matter of course, and the agent would have to make a decision to specifically not produce this data. An example of this would be someone buying a PC with an installed web browser configured to store and log all browsing behavior. The subject participates in the production of these logs without having to make any conscious choice to do so.

The accelerating diffusion of RFID technology into both commercial environments and state administered ID systems, is likely to lead to an increase in production of PII worldwide. Border agents and police in both China and the U.S. are already actively using RFID sweeping technologies to identify people of interest at national borders or in areas marked by social unrest.

#### HOW

There are many ways this question could be addressed that focus on the kinds of resources that are used, including people, technology, data, and formal procedures that play roles in the actual process of production.

Personally identifying information cannot be produced without first the act of identification. If, for example, a mediated interaction between a business and consumer is anonymous in the first place, the production of PII related to the transaction is highly unlikely. Identification may still be possible if the subject provides enough information about herself such that the combined attributes of descriptive identification are unique among the population, but this process is dependent upon the resources of the identifying agent or institution. An IP address alone is not likely to be transformed into a person's unique identity by Amazon.com, simply because the local ISP that may have this information has no reason to share it with them. Once a new visitor has registered as a customer, however, Amazon.com could potentially store that person's IP address associated with their name.

States, in this context, are likely to have the widest range of resources available to extract indexical identification from large amounts of descriptive information. Recently, for example, a FOIA request for information about records held in the Department of Homeland Security's Automated Targeting System (ATS) showed that the IP address of the individual making the plane reservation was stored by the commercial air carrier in its Passenger Name Record (PNR) and shared with the federal government (O'Neill, 2008). Without ubiquitous ID systems embedded into all of our common physical and virtual spaces, however, indexical identification is likely to take place when the deployment of limited resources is warranted, not as part of automatic dossier record production for all state subjects.

In China, in the traditional dossier system, the act of identification was so deeply embedded within the context — all the producers knew each other, usually quite intimately — that there was no need to pay attention to their particular identification technology (in this case their cognitive capacity to identify the individual they were writing about by face). As the production process has shifted from one, physical location, to a more distributed, mediated

process, the importance of identification as a necessary informational resource for the production of PII has grown. At the same time, ID systems have become an important site of struggle and potential resistance. While there is now a mandatory national ID card with a unique number for each citizen and the state encourages Internet users to register their activities and expression under their real names, there is a growing level of interest and appreciation for anonymity and privacy that is creating new opportunities for resistance to the state dossier system that were not present decades ago.

Even with the satisfactory ID of a subject individual, the actual production of a record of information is dependent upon a set of often standardized procedures. The production of a SAR report, for example, is detailed with the ISE SAR Standard and requires individuals in particular roles to make certain decisions and decide if the given information should continue upstream to a national database. A form, such as that filled out by a local *hukou* police officer in China, dictates that the officer enter particular categories of information, thus actively shaping the content, character and quality of the record.

#### WHEN?

It is possible to look at one in at least two ways when it comes to the production of personal information. First, when is the actual moment of production, the time at which this datum first comes into existence? If we are answering this question for a specific moment of production, such as when a given SAR containing PII about Sarah Q. Public, is recorded and stored in a local data system, this is better thought of as a specific site question. When becomes a question of logic when it dictates a particular calendar time when a record is to be produced. This production may be facilitated by the presentation of an ID token such as a national identity card, so we might ask at what times the state expects us to present ID. In addition to the specific time or moment of production, we can also ask how long the record will persist. What is the specific

data retention policy associated with this data? A specific “Time to Live” (TTL) may be embedded into the data object, either by code or simple policy, or it might persist indefinitely, sometimes sitting unnoticed in storage and at other times percolating through the dossier system.

Records produced within the culture of suspicion, as part of domestic intelligence rather than criminal cases, tend to have a much longer shelf-life than those attached to specific criminal investigations.

From a purely law enforcement perspective, if a lead is not deemed worth following, that is the end of the matter. For intelligence purposes, however, it might become a piece of information to be tucked away to see whether it is repeated or forms part of a later pattern. That is perhaps the sharpest difference between case-based law enforcement investigations and intelligence investigations. A traditional case-based approach to law enforcement investigation closes off alternative lines of analysis. Once a decision was made to go to trial, information that might emerge contradicting the theory of prosecution would not be ignored, but resources would no longer be devoted to a wide-ranging or exploratory investigation of the crime. The emphasis would be on seeking evidence to confirm one hypothesis (“Fred killed Jack”) and not on seeking information to confirm alternatives (“Mary is the killer,” or “Jack killed himself”). Intelligence, in contrast, constantly seeks different information to undermine, as well as to confirm, its preferred approaches. It is also eager to revisit past assumptions (Treverton, 2008, p. 18).

Many of the interlocking information systems which store and forward SARs in the U.S. have their own policies for how long records should be stored before being deleted, but this does not always reflect practice. Surveillance detection reports produced by Federal Air Marshals are stored within the Tactical Information Sharing System (TISS), for a period of 25 years. SARs produced and stored by local police departments, according to the current standard, are allowed to store them for up to 5 years. DOD TALON reports, SARs that were the subject of scandal in 2005-6 for reporting peace marches as threats, were supposed to be deleted from the reporting system within 90 days but remained long after.

Is there really a significant difference between “collecting” and “producing” information? This is not to deny that personal information is being collected, nor to argue that it is not important to seek ways to limit and these acts of collection. Instead, it is to bring attention to

aspects of the problem that may exist outside the perspective of this dominant frame, to bring attention to the contingent nature of our data shadows and data doubles and suggest leverage points for regulative policy. The process of collecting personal information is often not passive in relation to the record that is eventually stored. Paying attention to these moments helps us to understand how particular institutional and technological contexts shape the character and function of our evolving data doubles and data shadows. Once information is produced and stored by a private firm or government agency, restricting what happens subsequently to that data becomes considerably more difficult.

#### THE TARGETED PERSON

In the illustration to the right, there are four dossier model entities that interact with and reproduce one another.<sup>41</sup> Our key interest, what ultimately represents the basic human rights concern with the state dossier system, is the targeted person. The targeted person is ultimately produced and reduced by the state. It is produced in the sense that the person so named has a specific set of records —

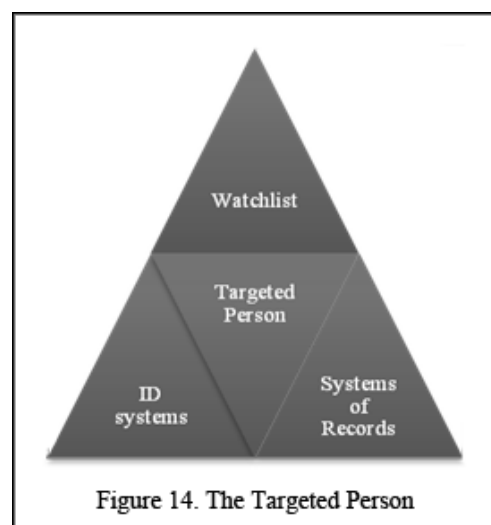


Figure 14. The Targeted Person

a dossier — produced and maintained within a state database. It is reduced in the sense that, when this specific data double is used to stand in for the subject, their life chances are constrained via subsequent state interference, justified via the legally inscrutable watch list.

This specific form of the term comes from the China case, where it refers to a sub-section of the Chinese population that receives the bulk of attention from state policing institutions. The targeted person, though it has many benefits for state bureaucracy, is an effective response to

<sup>41</sup> These are all key terms of art that were classified as "objects" in the linguistic toolkit (above).

limited state resources. Since the Chinese state does not have a police force of infinite size, and since individual police officers do not have unlimited mental and physical capacities to observe and report, the “targeted person” concept allows those resources to be concentrated where they are most effective. In the U.S., the term “person of interest” refers to someone under state observation, someone for whom the state likely has a detailed dossier to which certain state agents are actively referring. Although the term is often used in official statements to refer to individuals who have been named as an important suspect in a crime but who have yet to be charged (Richard Jewel, for example), it lacks an official legal definition. The growing phenomenon of the watch list is nothing less than the emergent classification of different “persons of interest” based upon why the state may be interested in them. Being a “person of interest,” leaves the subject absent significant legal recourse. It is a category worthy of more academic attention.

The role of “targeted people” in helping the state to manage limited resources is worth exploring in each individual case, and will likely change along with the evolution of technology and the social systems in which they are embedded. What is the particular logic of the targeted person classification? In other words, what is it that leads a state to identify a person as “targeted”? Are there resources for aggregating, storing and processing information so abundant that effectively the whole population is targeted and the distinction becomes moot? Or does the state begin to adopt an index of escalating attention categories, such that a greater set of resources are brought to bear as “interest value” increases?

## DEFENSE OF CLAIMS

The following table shows basic document types along the left-hand column with major, potentially controversial dissertation claims along the top row. Government documents and

investigative journalism, when propositionally in sync, afford credibility. The claim, for example, that the U.S. military spied on, created, and stored personal information on U.S. peace activists who presented no violent or criminal threat in 2005 (“Dossier Abuses”) is verified not just by MSNBC journalists but also by government documents including a U.S. DOD Inspector General report and a direct statement of DOD official to the press. The historical parallels under prior administrations in the 60s and early 70s are attested to not only by the epic scholarship of Donner but also by the highly detailed, publicly accessible congressional reports from the Church Committee.

Data Type	U.S.: Dossier Abuses	Few legal constraints	China: production transition	Anonymity gap	Rise of rights
Government Docs	X	X	X	X	X
Journalism	X	X		X	
NGO reports	X	X	X		X
Trade Press			X		
Western media	X	X	X	X	
Scholarship	X	X	X		X
Blogs	X	X	X	X	X

That China is undergoing a major transition in the sites and logics of state dossier production, yielding gaps of anonymity (“anonymity gap”) that appear to persist despite the government’s clear desire to eliminate them, and that these gaps are not necessarily qualitatively



inferior to similar gaps in the U.S., is a complex claim comprising a set of propositions which may each be defended based on multiple, triangulating source types. I established the original sites and logics of dossier production in China on the basis of extant China studies scholarship and state run media, which serve as two key anchors for triangulation. Data speaking to the ongoing transition of the dossier system, both technological and bureaucratic, was drawn from state run media, academic scholarship, and authoritative blogs.

#### COMPARABILITY OF U.S. AND CHINA

Perhaps the most radical claim in this dissertation is that the Chinese and U.S. dossier systems are in fact comparable. Given the dramatically different governmental structures and socio-political histories of the two countries, how can we begin to pretend that particular laws are in anyway comparable, or that the expression of the dossier system as a tool of oppression, or the power of the people to resist can be within even the same order of magnitude? Dossiers are bureaucratic technologies that function across the political spectrum; they are tools of government (Hood, 1983; Hood & Margetts, 2007), instruments for gathering information and affecting behavior at the point where the state comes into contact with citizens.

The fact that a common set of language tools emerged from the study of the two cases, and can be used to talk efficiently about them, is a powerful testament to at least some level of comparability. Both states have an interest in ID and record systems and both have identifiable sites and logics of record production, as well as one or more classes, groupings, categorizations of people who deserve heightened scrutiny and attention. Both are subject to the bounded rationality of institutions and the individuals that comprise them. Both have states and corresponding publics who may object to a certain dossier system policy and both have responded to and rejected these demands in different instances. Both states have powerful actors circulate measures of public opinion as part of the ongoing negotiation between state and public interests.

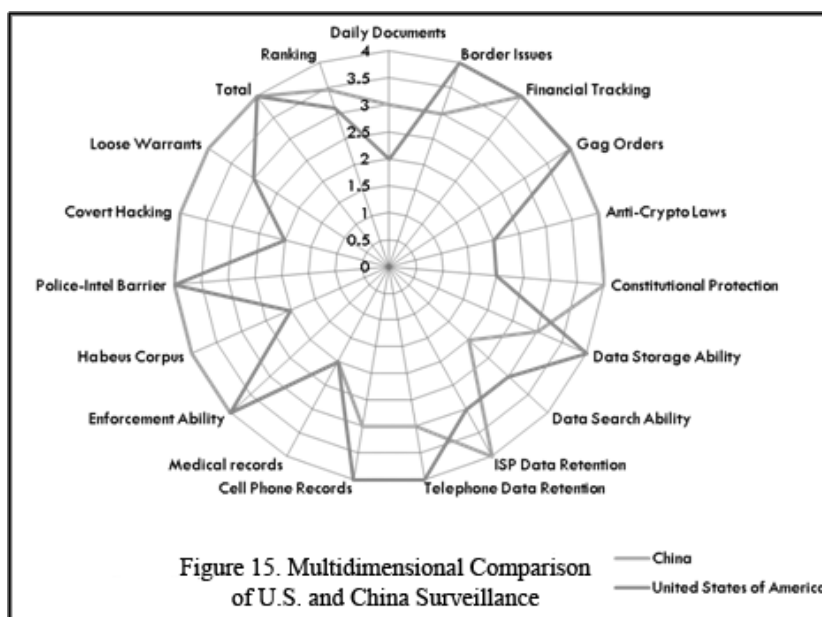
The most direct independent correlation with this particular proposition comes from the research work of two organizations now doing global rankings of surveillance regimes on an annual basis: Privacy International and Cryptohippie, Inc.. Privacy International, in cooperation with the Electronic Privacy Information Center (EPIC) in Washington, began to release annual global privacy rankings beginning with the year 2006. Based primarily on data produced in its annual privacy and human rights (PHR) report, which itself is gathered via both publicly available documents and a network of area experts,<sup>42</sup> the rankings for 2006 were broken down according to thirteen categories, including “constitutional protection,” “identity cards and biometrics,” and “communication data retention.” Countries received a numeric score from 1 to 5, with 1 representing the most negative, privacy-free state, the “endemic surveillance society” (ESS). In both 2006 and 2007, China was ranked as an ESS, posting the worst overall score (1.3) along with Malaysia and Russia. The U.S. was not far behind. In 2006, the U.S. overall score was 2.0, putting it in the second worst category of “extensive surveillance society.” In 2007, its score dropped to 1.5, moving it into the class of “endemic surveillance society” shared with Russia, China and Malaysia.

For 2008, a separate organization, Cryptohippie, Inc., without describing its methodology, released its own ranking based on seventeen factors, many of them similar to Privacy International. According to Cryptohippie, the U.S. ranked worse than China in five categories: “border issues,” “data storage ability,” “data search ability,” “telephone data retention” and “cell phone records.” While China was worse in seven categories, including “daily documents,” “constitutional protection,” “ISP data retention,” and “habeas corpus.”

---

<sup>42</sup> I participated in research process for PHR 2005 as an EPIC law clerk.

Before continuing, it is important to recognize that the intention of Privacy International and Cryptohippie was to compare nation states in terms of surveillance and privacy and not the narrower formulation of dossiers that is the subject of this dissertation. In many cases this distinction is not significant, such as when the specific criterion of comparison deals with an issue of identification systems or communications data retention. In other cases, the ranking may make



sense if one is thinking about surveillance in general, which includes constraints on the state's capacity for real time surveillance, but might look different if one is focusing on the state's capacity to produce and aggregate records of personal information. If we look specifically at the practice of state dossier systems, the U.S. may currently rank as more extreme than China.

While it is understandable that both Privacy International and Cryptohippie both show China with less constitutional protection against state surveillance than the U.S., these constitutional protections are much less significant if the focus is on dossier systems. As I have described earlier, the distinction between information in storage and that in transmission renders much personal data outside of the boundary of the Fourth Amendment, at least as currently interpreted by the courts.

In the comparative ranking on identification cards and biometrics, Cryptohippie's 2008 ranking shows China as worse than the U.S. while Privacy International showed the two countries' shifting positions in 2006 and 2007. While China was ranked worse in 2006, (2 to 3), the U.S. dropped to the worst possible score (1) for 2007 while China's score remained the same. Is it possible that conditions changed again in 2008 or were the two studies based on different functional definitions of these categories and/or differing data? Cryptohippie's definition of its "Daily Documents" category is "Requirement of state-issued identity documents and registration." Privacy International has an extensive note explaining its "Identity card and biometrics" category:

We assessed the extent and nature of identification practices and proposals in each country, including data sharing between identity and other systems. Any requirement in legislation to present identity was also taken into account, as was any requirement in law to disclose biometric data. The development of conventional elements of enforced compulsory identity schemes was also taken into account. These include national identity registers, national numbering systems, national identity cards, the establishment of legal obligations to disclose personal data and the creation of new crimes and penalties to enforce compliance with legislation. (p. 5)

Looking on the surface of the national ID issue, it is easy to see how one might come to the conclusion that China's system is worse than the U.S.. After all, China has a mandatory national ID card with an embedded RFID chip that residents are required by law to carry, while the U.S. Real ID initiative to implement national standards for state driver's licenses appears to have been soundly rejected on the basis of both cost and human rights concerns. Deeper investigation, as I have shown, yields a different picture. Further, while the Chinese law officially requires citizens to carry the national ID at all times, the law is not enforced. Most Chinese do not carry the ID with them. In the U.S., on the other hand, most Americans carry their driver's license with them at all times, in part due to the legal requirement that you carry your license whenever you drive.

Although it ranks China worse in Constitutional privacy protections, Privacy International, for both 2006 and 2007, has ranked the U.S. worse than China in terms of statutory privacy protections. As I explained in the historical and legal context chapter for the U.S. case, there is a bright line distinction in U.S. law between information that is in transmission and that in storage. Since these global rankings are based on the more general definition of surveillance and statutory law is in general more specifically targeted than constitutional law, we cannot simply assume that the comparison would be the same.

## CONCLUDING THOUGHTS

There has been a tendency in recent surveillance scholarship to dismiss the power of the state to put itself at the panoptic center of the global surveillance matrix. So many acts of surveillance and monitoring are going on in so many contexts by so many actors that it would be absurd to assert that the state can somehow be at the center of all of it. It is indeed a “surveillant assemblage.” Personal records that persist, however, are distinct from real-time surveillance. Personal records can flow over time from system to system and state institutions tend to have a much higher “document gravity” than private institutions. The state has unique authority to demand that an individual or private institution provide information or surrender a particular document, even the power to seize a document. States have unique power to interfere with the lives of their subjects and unique power to constrain or afford the process of dossier production. The state also has unique authority to act physically on personal information that they attend to. From democracies to authoritarian regimes, states can and do take authority to regulate the private sector, to varying effect. Individual corporations cannot pass laws affecting everyone within a particular national border. This power must be continually scrutinized. When exercised to excess, authoritarian and even totalitarian scenarios become more likely. In other words, they are afforded by the very presence of widespread dossiers on large sectors of the population. As

Arendt (1951) reminds us, the never ending struggle against totalitarianism has determined the very existence of politics.

#### SUSPECT UNTIL PROVEN GUILTY

Watch lists and SARs in the ISE create an environment of perpetual suspicion. Under the legal cloak of domestic intelligence operations, reports on our potentially threatening actions will be logged, stored, circulated and re-circulated, feeding into a progression of commercial (off-the-shelf) and specially developed data mining algorithms to categorize the “risky” subject, with growing numbers of completely innocent citizens finding themselves subject to harassment, detention, or worse. Basic suspicion becomes the state’s defense for collecting or producing a particular record on a target subject, but the record persists and at a later date may fuel more suspicion, and thus the generation of new suspicious activity reports, in a potentially never-ending vicious cycle. Citizen subjects under such a system will become quite literally “suspect until proven guilty.”

The public must constantly scrutinize the PII production logic of the state. Under the Total Information Awareness program the U.S. has argued that it must produce as much information as possible, that from such high volumes of data the patterns of terrorists can be discovered. They can be isolated apprehended and dealt with prior to their actually committing their planned act of terror. This logic, however, has been vigorously challenged in the academy (Chakrabarti & Strauss, 2002; Martonosi & Barnett, 2006; Jonas & Harper, 2006). In its 2008 report, the National Research Council summarized some of the critiques:

Modern data collection and analysis techniques have had remarkable success in solving information-related problems in the commercial sector; for example, they have been successfully applied to detect consumer fraud. But such highly automated tools and techniques cannot be easily applied to the much more difficult problem of detecting and preempting a terrorist attack, and success in doing so may not be possible at all. ...

Automated identification of terrorists through data mining (or any other known methodology) is neither feasible as an objective nor desirable as a goal of technology development efforts...

Because data of questionable quality are likely to be the norm in counterterrorism, analysts must be cognizant of their effects, especially in fused or linked databases, and officials must carefully consider the consequent likelihood of false positives and privacy intrusions. ("Protecting Individual Privacy," 2008, pp. 2-4)

A recent conference paper produced under a DARPA research grant, however, argues that critiques of "information awareness systems" are overly simplistic and often contain unfounded assumptions (Jensen, Rattigan & Hannah, 2003). For example, most mathematical critiques, the paper asserts, assume that the system produces only binary decisions (terrorist or non-terrorist) rather than a graded scale of values.

Increased attention should be given to the logic of both individual record systems and the more general logic driving the domestic intelligence system as a whole, as overproduction can have significant impact on the life chances of individuals. Under the emerging configuration of the ISE, it appears likely that documents will continue to be produced for many reasons unrelated to the war on terror or even the fight against crime. The producing state agent may be attempting to meet a quota or avoid a fine, or, based on literature provided to them by their local fusion center or national threat reporting center, they may conclude that the possession of particular political documents indicates likely "domestic terror" associations.

#### BOUNDARY RESOURCES V. CONNECTING THE DOTS

The change in the production and role of records of personal information in the United States has been quite dramatic since the September 11<sup>th</sup> attacks. Quite clearly, the principles of state policy designed to constrain the production of official and quasi-official documentation of suspicion via the practice of domestic intelligence have been largely reversed. The state appears to have taken the position that boundary resources of any kind are toxic to the nation's security.

The notion of “anonymity” online, for example, has no real place during the 21<sup>st</sup> century war on terror. In October, 2008, Donald Kerr, the principal deputy director of U.S. national intelligence, told a conference audience in San Antonio, Texas that anonymity is now an anachronism:

[I]n our interconnected and wireless world, anonymity - or the appearance of anonymity - is quickly becoming a thing of the past.

Anonymity results from a lack of identifying features. Nowadays, when so much correlated data is collected and available — and I’m just talking about profiles on MySpace, Facebook, YouTube here — the set of identifiable features has grown beyond where most of us can comprehend. We need to move beyond the construct that equates anonymity with privacy and focus more on how we can protect essential privacy in this interconnected environment.

Protecting anonymity isn’t a fight that can be won. Anyone that’s typed in their name on Google understands that. Instead, privacy, I would offer, is a system of laws, rules, and customs with an infrastructure of Inspectors General, oversight committees, and privacy boards on which our intelligence community commitment is based and measured.

Kerr is essentially saying that we should be focusing now on how the government will safeguard the data it has on us, rather than questioning its right to have it.

Physical boundary resources once available to us in relative abundance (the walls of a study, the locked drawer, an isolated house) have become less useful in the current mode of electronic networked communication. The Chinese, who, for example, have more recently experienced the novel value of private bedrooms as a valuable boundary resource, and who have suffered for decades under the particularly weighty and comprehensive traditional state dossier system, may be more motivated to see that boundary resources can be logically transferred to 21<sup>st</sup> century social systems.

As we react to these changes, we can develop new schema that provide new kinds of boundary resources — soft logical resources such as language and metaphor, or harder resources like law and code. It is critical that western privacy activists recognize the value in continued and expanded dialog with Chinese actors in the state and public.



## DOSSIER SYSTEMS AND THE CONTEXTUAL INTEGRITY OF PERSONAL INFORMATION

Within the context of the SDS as a problem, it becomes vitally important whether what is being produced is contextual indexical information (see chapter 2, p. 45) or de-contextualized with a unique, persistent identifier. The persistent identity is the physical person upon which the state, on its own authority, may ultimately act. For most businesses, especially modern, mediated business, they may very well never see their customer and their specific real, physical identity is often never of concern. For a state's action against a citizen to be just, they must be defensible via the presentation of some dossier identity, a set of propositions about the whereabouts and actions of a specific, persistent individual.

It is quite possible to develop an infrastructure for electronically mediated commerce where data doubles do not contain personally identifying information, where they can contribute to better customer service and convenience without necessarily adding weight to the individual's data shadow. Consider, for example, an online bookseller's customer database with contextual indexical identifiers. The customer invokes the identifier with something only they know, such as a username and password. When the system receives this unique set of logon credentials it then associates the entity's browsing and purchase behavior with this contextual identifier, putting the customer in control of this data double and thus allowing them to contribute personal information without adding to the stock of personally identifying information about them. It is possible to isolate both payment and shipping systems, which do require indexical identification, without facilitating the combination of this data.

In the case of Suspicious Activity Reports, certain basic policy changes could maintain the primary goal of the report system while protecting innocent people from unnecessary government intervention in their lives. By focusing on the activity rather than the person, SARs

can provide police and military important intelligence to be on the alert for particular types of behavior that are clearly threatening without needlessly implicating innocent individuals in groundless witch hunts.

#### DOSSIER SYSTEMS AND THE CYBERNETIC DEFINITION OF SURVEILLANCE

Under the original definition of surveillance that informs this dissertation, I point out that the personal information flowing back to the state is really only significant if it leads to the state acting in some way that impacts an individual's life. We know from history that as state ID and record systems become more pervasive and less tolerant of the contextual integrity of its people's private lives, the public interest suffers. Nevertheless, given that the U.S. has had a full-fledged state dossier system for several years now, one would expect to see signs of an emergent friction at the interface between state agents and the public. While this has not been the focus of this dissertation, signs of political oppression are increasingly obvious.

On Oct 23, 2001, FBI agents visited San Francisco retiree Barry Rheingold to question him about his political views shortly after he complained while watching a television report at his local gym, "[t]his war is not just about getting terrorists, [i]t's also about money and corporate oil profits." On October 26, 2001 FBI agents visited the home of a college freshman in North Carolina to investigate the report of an "un-American poster" on display in her home (Chang, 2002). While these incidents occurred very soon after 9/11 and may be excused as excesses arising out of the moment, the interference in what must fairly be described in the political lives of Americans has continued and even expanded in the 8 years since, in a manner highly reminiscent of phase 1 of U.S. dossier history.

In 2005 and 2006, Maryland State Police built intelligence files on numerous people engaged in First Amendment activities of speech and assembly with no demonstrable or

conceivable connection to domestic terrorism. Files included personal details on activists for Amnesty International, the NAACP, the Campaign to End the Death Penalty, the International Socialist Organization, and United Catholic Charities. According to the ACLU of Maryland:

Agents collectively spent at least 288 hours on their surveillance over the 14-month period in 2005 and 2006, the ACLU of Maryland says. Agents “monitored private organizing meetings, public forums, and events held in several churches, as well as anti-death penalty rallies outside the state’s SuperMax facility and in Lawyer’s Mall in Annapolis.”

Although Maryland Police admitted that more than 50 people engaged in non-violent, peaceful speech and assembly were categorized as terrorists in a state database that was made accessible to federal agencies, more recent revelations suggest that numbers were much higher. The effect of this kind of state police operation is hard to ignore. Wanting to avoid the hassle that comes with appearing on a federal terrorism database, some people ratchet down their activity. Jennifer Flynn, an AIDS activist in New York who was actively monitored in public by what appeared to be unidentified state agents, describes her and her associates’ feelings that have followed this increase in scrutiny:

“I feel like I’ve stepped back, in a way,” she says. “I feel I’m not as vocal as I was. I’m still going to sign a petition. I’m still going to organize a rally. I do it. But now I’m deathly afraid.”

...

Flynn says the damage is done. She sees it in the attitudes of other activists. There’s less desire. More trepidation.

“When you use scare tactics, you really are curbing our right to dissent against the government,” she said. “The only thing this is serving to do is squash public dissent. By going after the organizers of a rally, you really are sending a message – ‘Don’t hold a rally.’” (Parascandola, 2007,n.p.)

With increasing frequency, U.S. citizen activists and academics critical of the U.S. government are finding that they have lost their freedom to travel:

Jan Adams and Rebecca Gordon, American peace activists, tried to check in at the San Francisco airport for a trip to Boston in August 2002. Airport personnel who said that these middle-aged women were on the “master list” called the police and notified the FBI. At least twenty other peace activists are confirmed to be on the list: A 74-year-old catholic nun who works for peace was detained in Milwaukee; Nancy Oden, a leader of the Green party, was prevented from flying from Maine to Chicago. Free speech advocates are on the list: King Downing of the ACLU was detained in the Boston airport in 2003. David Fathi, also of the ACLU, was detained as well. Scholars who defend the Constitution are on the list: in 2007, Professor Walter F. Murphy, emeritus of Princeton, one of the nation’s foremost Constitutional scholars, who had recently spoken critically of Bush’s assault on the Constitution, was detained for being on a “watch list.” A TSA official confirmed informally that it was probably because Murphy had criticized the President, and warned him that his luggage would be ransacked. (Wolf, 2007, pp. 95-6)

In addition to negatively impacting the lives of innocent American citizens, too much PII flowing towards central state policing institutions begins to choke information systems designed to provide early warning of criminal and terrorist acts, increasing the rate of “false positives” and thus squandering limited resources. In order to properly regulate the level of PII production, policy analysts must carefully consider the “whys” and “hows” of PII production. If there is a claimed use from a particular moment of production, is the given explanation logical? Is the PII produced for exchange, legal requirement or technological affordance without a clear use value? If “use value” is claimed by the particular producers, does the claim withstand scrutiny? How do we design ID systems to limit the production of PII? Focusing on authentication rather identification unless there is a justifiable need is clearly one way to do this.

As privacy advocates take stock of the rapidly developing global surveillance state, it will behoove them to understand that, from a policy perspective, the moment of production has multiple points of leverage. After the fact, the situation quickly becomes intractable. Personally identifying information does not simply exist out there to be collected and distributed. Its existence is contingent upon institutional, economic, and technological contexts that are very much within the regulatory domain of policy. If instead, we take the ongoing explosion of

personally identifying information, the growing weight of our collective data shadow, as a natural phenomenon outside our control, we become complicit in our own incapacitation.

... because and insofar as people consider social facts as things, because and insofar as they experience and describe them as natural, failing to recognize that they casually reconfirm their matter-of-factness and transcendent singularity, they rebound upon individuals with the force of things, which carry real and hard consequences for their every day behavior. (Pels, 2002, p. 73)

It would be difficult, based on the data gathered during this research, to make a definitive statement on which of the two countries has stronger constraints on the emergence of a totalitarian dossier system. This should call attention to the seriousness of the current configuration and developing trends within the U.S. system, while at the same time offering hope of resistance within what may appear to be very different political systems with different expectations about the power of popular will.

## APPENDIX A: SEARCHING FOR THE MOTHER OF ALL DATABASES

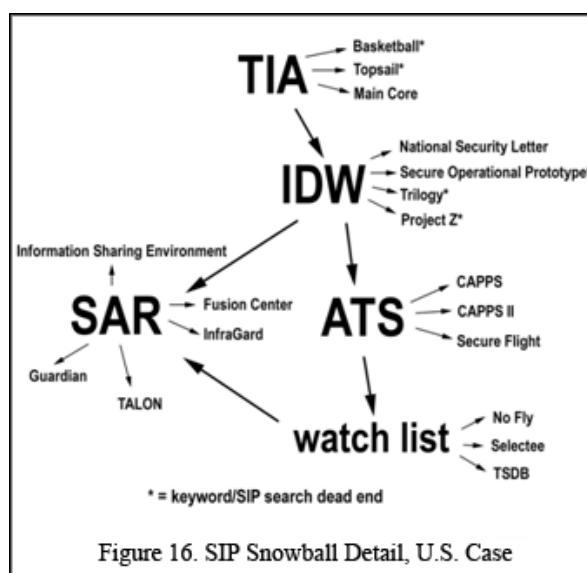
### (RESEARCH NOTE)

The state must collect a wide range of personal information and the volume and quality of this information directly impacts the state's capacity to serve the public interest. It is important, however, that these individual systems remain separate enough so that the information contained within them maintains its contextual integrity. In other words, the data should be tightly bound to the particular institutional service: unemployment, health insurance, crime control. To avoid the risks associated with totalitarian regimes, it is important that these individual systems have sufficient enough distribution of boundary resources (Altman, 1981) — be they laws, technology, or cultural norms — so that citizens have spaces to experiment and play with their own identities. Record systems must remain separate enough so that it would be simply inaccurate to speak of them as a “state dossier system,” or in more Kafkaesque terms, a Mother of All Databases (MOAD).

That China has a MOAD is not a controversial proposition. There is no doubt much more to the system than the national population registry described in chapter 6, but that it exists is beyond dispute. According to U.S. law, the federal government cannot maintain such a system. This, after all, was the main purpose of the Privacy Act. Given the very different post-9/11 world and the state's claim to surveillance capacity for national security, a committed SDS researcher obviously starts off with this question. Does the U.S. have a single, massive database (system of records), containing broad and detailed information on every citizen? The question does not have a simple yes or no answer.

I have gathered and analyzed a very large volume of data, government documents, congressional testimony, mass media, and NGO reports. I have set no preconceived boundaries on the type of data that I might consider; only that I encounter the document within the semantic boundaries established as part of the state dossier system (SDS) problem frame. Data retention focused primarily on the state rather than private actors and avoided selecting particular institutions or well known system of records (SoRs) as the starting point for research. At first, these boundaries were very broad, consisting of keyword sets like “united states,” “surveillance” and “database” but later evolved into more directed searches, more specific keyword sets and identified SIPs (statistically improbable phrases) that were used for RSS feeds and online database queries (e.g. Investigative Data Warehouse, fusion center, InfraGard). While the real-time RSS data feed was refined over time, the most significant changes were made at the archival search level, as I sorted through particular nodes of interest and evolved a reference list of the most significant SIPs and one word terms via a process I call “SIP snowball sampling.” To review, this method is used to navigate the large extent data set of SDS-related records via the notation of significant names and phrases and then conducting further archival searches with these phrases (SIPs) as keywords.

The figure (16) to the right provides a more detailed view of SIP progression for the SoR component of the U.S. SDS case study. To simplify this illustration, I focus on SoR names and a handful of proto-institutions (fusion centers, InfraGard), while leaving out other terms that were encountered in the course



of research such as laws, established institutions, and the names of private firms. Since I was approaching the U.S. case from the very general state dossier frame, my initial question related to whether or not the U.S. had a single database containing detailed information on all U.S. citizens, a single Mother of All Databases (MOAD), similar to China's population registry. Total Information Awareness (TIA) became the initial, focal SIP for research, as it has been the most salient phrase, the most closely connected term within current or recent public discourse related to the MOAD question since its initial appearance and seemingly short life in 2002. As I actively gathered investigative reporting, congressional testimony, and other government documents containing the TIA SIP, a number of realizations became clear. First, that the TIA program continued after being defunded by Congress in everything but name. Second, that the new names under which these programs proceeded were so generic as to insure they would be lost in a sea of search noise — names like “basketball” and “topsail.” During this research phase, other candidates for the MOADB, with history going back decades prior to the September 11<sup>th</sup> Attacks, came to light.

Dating back to the 1980s and known to government insiders as “Main Core,” this poorly (publicly) documented SoR reportedly collects and stores — without warrants or court orders — the names and detailed data of Americans considered to be threats to national security. According to several former U.S. government officials with extensive knowledge of intelligence operations, Main Core in its current incarnation apparently contains a vast amount of personal data on Americans, including NSA intercepts of bank and credit card transactions and the results of surveillance efforts by the FBI, the CIA and other agencies. One former intelligence official described Main Core as “an emergency internal security database system” designed for use by the military in the event of a national catastrophe, a suspension of the Constitution or the imposition of martial law. Its name, he says, is derived from the fact that it contains “copies of the ‘main



core’ or essence of each item of intelligence information on Americans produced by the FBI and the other agencies of the U.S. intelligence community” (Shorrock, 2008, n.p.).

The reality of such a system is always elusive, however, and unlikely to yield to even the most intensive examination of publicly available documents. Shorrock’s sources were former intelligence officials, not publicly available texts. There are no official documents, no Systems of Record Notices in the *Federal Register*, no Privacy Impact Assessments, no Justice Department Inspector General reports accessible to the general researcher attesting to the existence of “Main Core,” and so continuing to focus on this SIP is not a particularly good fit for the chosen method.

Another SIP, “Investigative Data Warehouse (IDW),” emerged as a more practical candidate for a MOAD, as its existence was attested to by not only investigative reporters but also by its home institution, the FBI in the form of congressional testimony and well-reported public press conferences. The IDW was clearly a significant SoR that contained a massive amount of information on American citizens with no criminal record. Although the FBI was publicly demonstrating IDW, public information about it was limited. Further, it became clear that many government officials responsible for either managing or overseeing the data warehousing project had difficulty agreeing just what they were talking about. That is, the name, the indexical identifier, the SIP, for this particular SoR, always remained somewhat cloudy. To illustrate, below are a series of exchanges that occurred during congressional hearings focusing on the need for a new all encompassing information architecture at the FBI to better fight the threat of terrorism. The names of SoRs and related IT initiatives are underlined:

MUELLER: We have been an organization with stovepipes. Each division had their own computers four years ago; different software packages. We have an overarching architecture now, and it’s important for us that when we come up with a new software, a piece of software, piece of hardware, that it is approved by the CIO and it fits into the overarching architecture.

And so I am going away from, sort of, looking at this project as a monolithic project that's going to be 39 months. It's going to be iterative project. It will have a number of components that will address not just our case management system, but other areas where we need to upgrade our IT.

MOLLOHAN: Increasing capability as you go along. Are you still calling this virtual case file?

MUELLER: No.

MOLLOHAN: What are you calling it?

MUELLER: We are looking for names. We've had Trilogy and virtual case file that have dominated our thinking for the last three and a half years, and the latest thing I saw here was Project Z, but I'm not certain that I want to go with Project Z. [p. 582]

MS. BAGINSKI: We can, in fact, in the Investigative Data Warehouse, which actually started out as something called the Secure Operational Prototype. It was all based on terrorism. We can do the string that you're talking about, the multiple word.

SEN. LEAHY: You can do that in Tri — ?

MS. BAGINSKI: In Trilogy, is that what you mean, sir?

SEN. LEAHY: In Trilogy, yeah.

MS. BAGINSKI: IDW is actually something that I would call separate from the Trilogy package that you guys, you and I have been talking about.

SEN. LEAHY: Could you do it in Trilogy though?

MS. BAGINSKI: Trilogy is not a data warehouse that you would search against. That's why I'm having the trouble answering the question. Trilogy is hardware, as you pointed out, desk — you know, computers and desktops, local area networks, wide area networks for the connectivity. And it is the case management application. The case management application then feeds the integrated data warehouse that I'm describing. That allows me to do your search. [p. 525]

LEAHY: Thank you. During the May 2 oversight hearing, you testified about the investigative data warehouse, IDW.

MUELLER: Yes.

LEAHY: This was put up after 9/11. It now contains over half a billion FBI and other agency documents. Nearly 12,000 users — federal, state, local law enforcement — can access through the FBI network. Now, I've long advocated they use technology in the FBI to carry out your programs. But I'm worried, partly because I read about the ATS program and the data-mining: Does this have adequate security? Does the IDW database share information or otherwise interface with the ATS data-mining program?

MUELLER: The ATS data-mining program? I'm not familiar with what you're referring to, sir.

LEAHY: Just talking about the ATS.

MUELLER: You mean DHS?

LEAHY: The DHS — well, they call it ATS. I realize we're using acronyms, but this is the one that checks on everybody crossing our borders. And you have the Department of Homeland Security's automated targeting system.

Does your database interface with that? Does it share information with it?

MUELLER: I do not believe so. But, again, I would have to go back and check. I do not believe so.

LEAHY: Well, this is very important to me. I wish you could get back to me in the next few days...

MUELLER: Will do so.

LEAHY: ... and let me know directly. [p. 549]

No one, not high level officials at the FBI, not senior members of the Senate Committee on Foreign Intelligence, seem to know just what name to call the FBI's data warehousing project. As research continued, it became clear that searching for the name of the posited Mother of All Databases (MOAD) is something akin to seeking the true name of God. For a researcher attempting to understand the configuration of the U.S. Dossier System, this poses an interesting problem. Without having a consistent name or label to apply to a subject of interest, gathering data which speaks to it becomes much more than a simple, directed keyword search. The SIP snowball method provides a way to continue gathering data while remaining open to important new directions.

Even if one chooses to work at a lower level of individual, smaller scale SoRs that are mentioned within Privacy Act SORNs and E-Government Act PIAs and appear to contribute significantly to the overall configuration of the U.S. dossier system, these record systems appear to number in the hundreds. A 2007 report published by the DHS Privacy Office noted that DHS, since its inception as a government agency, has published 51 System of Records Notices (SORNs) announcing new or planned record systems per requirements of the Privacy Act and

was processing an additional 207 legacy SORNs that needed to be reviewed and either re-published or retired (Teufel, 2007). According to a 2004 survey of 128 federal agencies and departments,<sup>43</sup> the GAO identified 122 separate data mining projects involving the collection and analysis of personal information.

A study by the RAND Corporation of the U.S. domestic intelligence system maps the number and complexity of the interlocking data systems that comprise the U.S. domestic intelligence apparatus. Virtually all of the SoRs, of which there are more than 50 in the chart, contain PII on U.S. citizens. In addition to the IDW, large-scale SoRs of significant interest to the SDS problem frame include Analysis, Dissemination, Visualization, Insight and Semantic Enhancement (ADVISE), OneDOJ, the National Crime Information Center (NCIC), the DOD's Joint Protection Enterprise (JPEN) system, the Treasury Department's Treasury Enforcement Communications System (TECS) and Financial Crimes Enforcement Network (FINCEN), and the IRS's REVEAL system. Some of these programs have been shut down and then replaced by similar or identical programs with different names. ADVISE, for example, was shut down after unfavorable comments in the public about the way it echoed the "forbidden" TIA program, but was soon replaced with another initiative, the System to Assess Risk (STAR) (Nakashima, 2007). The JPEN system was shut down in 2007 with most of its functions absorbed by the FBI's Guardian system.

To recap, the number of U.S. government databases containing significant amounts of PII is large and systems often change their name. Further, as impressive as the RAND chart might be, it barely scratches the surface of key SoRs within the U.S. state dossier system, as a very large number of databases are in private hands or within government IT systems that, because of their

---

<sup>43</sup> The CIA, NSA and the Department of the Army, DOD, did not respond.

national security or law enforcement role, are excluded from Privacy Act or E-Government Act reporting requirements.

While important to the understanding of the U.S. dossier system, it quickly became apparent that relying on the SoR as the primary lens for data gathering, at least within this U.S. case, would not necessarily yield a broad enough picture of the problem. As a result, in later stages of data gathering and analysis I began to pay more attention to SIPs that fell at a lower level of analysis than specific SoRs. In other words, I began to focus more on types of records than on specific database systems. I identified two types of records — suspicious activity reports (SARs) and watch lists — as particularly important and problematic components of the U.S. SDS with potentially even more serious interactions.

## APPENDIX B: DOCUMENT SOURCE BREAKDOWN

**Overall:** data is broken down into the following seven overall categories.

- 1) government documents
- 2) investigative journalism
- 3) NGO reports
- 4) trade press
- 5) western media
- 6) academic scholarship
- 7) authoritative blogs

Below, I break down the categories in some more detail for the U.S. and China case studies.

### U.S. CASE

**Government Documents:** Includes laws, privacy impact assessments (PIAs), systems of records notices (SORNs), Inspector General reports, congressional testimony, notices of proposed rulemaking (NPRMs), memos, and other documentation from multiple departments and agencies including the U.S. Government Accountability Office (GAO), U.S. Congress, Department of Defense (DOD), Department of Justice (DOJ), Department of Homeland Security (DHS), Federal and State courts, and the Program manager for the Information Sharing Environment (PM-ISE).

**Investigative journalism:** Rothschild's work on Infragard & TLO; Single, R. on Real ID; Pincus on TALON; Shorrock on Main Core.

**NGO reports:** American Civil Liberties Union (ACLU), Electronic Privacy Information Center (EPIC), Center for Democracy and Technology (CDT), Privacy International, Cato Institute, Federation of American Scientists (FAS) and the Electronic Frontier Foundation (EFF)

**Trade press:** *Federal Computer Week, IEEE Security & Privacy, IEEE Intelligent Systems, Business Week, Physorg.com, RFIDNews, Washington Technology, Security Focus.com, AIMGlobal, Security Focus, Government Technology, Bank Rate.com, Forbes, Security Management, E-Commerce Times*

**Western media:** *NYT, Washington Post, MSNBC, Christina Science Monitor, USA Today, St. Louis Dispatch, CQ.com*

**Academic research texts:** books and journal articles in the following areas: Surveillance Studies, Privacy, U.S. intelligence history, U.S. law. Cited law journals include: *John Marshall Journal of Computer Information and Law, Harvard Law Review, UCLA*

*Pacific Basin Law Journal, Yale Law Journal, Boston University International Law Journal, Stanford Law Review, Cornell International Law Journal, Georgia Law Review, Boston University Journal of Science & Technology Law, NYU Law Review, Southern California Law Review.*

## CHINA CASE

**Government documents:** Primarily state run media, national, including the *People's Daily*, *China Daily*, and *Beijing Review*, and regional such as the *Southern Weekend* (Nanfang Zhoumou) and the *Shanghai Star*. Also the texts of national laws and other relevant documents in the public domain, such as those from court cases.

**NGO Reports:** *Privacy International, Human Rights Watch, Duihua Foundation, Reporters without Borders*

**Trade Press:** *China IT & Telecom, China Leadership Monitor, China Economic Review, China Business News Online, Pacific Epoch.com, Printed Electronics World*

**Western media:** *NYT, Washington Post, Christian Science Monitor, AP, UPI, Business Week, BBC*

**Academic:** China studies scholarship in books and journals, including: *The China Quarterly, China Leadership Monitor, Chinese Journal of International Law, Journal of Public Policy*, and *Journal of International Affairs*. Major books and articles covering: privacy and human rights, the hukou system, and the national ID card.

**Authoritative blogs:** the China Media Project, EastWest-North-South, Rebecca McKinnon, Global Voices Online, China Law Blog, Danwei.org

## REFERENCES

- 68 Fed. Reg. 45265 (2003, August 1). Subject: Passenger and Aviation Security Screening Records to support the development of a new version of the Computer Assisted Passenger Prescreening System, or CAPPS II. U.S. Department of Homeland Security (DHS), Transportation Security Administration (TSA). Notice of status of system of records; Interim final notice; Request for further comments.
- 68 Fed. Reg. 55593 (2003, September 26). Subject: Joint protection enterprise network. U.S. Department of Defense (DOD), the Joint Staff. Notice to add a system of records.
- 71 Fed. Reg. 60928 (2006, October 17). Subject: Card Format Passport; Changes to Passport Fee Schedule. U.S. Department of State (DOS). Notice of proposed rulemaking. 22 CFR Parts 22 and 51, RIN 1400–AC22 [Public Notice 5558]
- 71 64543 Fed. Reg. (2006, November 2). Subject: Automated targeting system (ATS) -- DHS/CBP. U.S. Department of Homeland Security (DHS), Office of the Secretary. Notice of Privacy Act system of records. [DHS-2006-0060]
- 72 Fed. Reg. 10820 (2007, March 9). Subject: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes. U.S. Department of Homeland Security (DHS). Notice of proposed rulemaking. 6 CFR Part 37 [Docket No. DHS–2006–0030] RIN 1601–AA37.
- 72 Fed. Reg. 74169 (2007, December 31). Subject: Card format passport; changes to passport fee schedule. U.S. Department of State (DOS). Final rule.
- 73 Fed. Reg. 5271 (2008, January 29). Subject: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purpose. Final Rules. 6



- CFR Part 37 [Docket No. DHS–2006–0030] RIN 1601-AA37. U.S. Department of Homeland Security (DHS).
- 51% say security more important than privacy. (2008). Retrieved March 5, 2008, from [http://rasmussenreports.com/public\\_content/politics/current\\_events/general\\_current\\_events/51\\_say\\_security\\_more\\_important\\_than\\_privacy](http://rasmussenreports.com/public_content/politics/current_events/general_current_events/51_say_security_more_important_than_privacy)
- 84 days and nights in Guangzhou. Retrieved 11/13/2007 from <http://www.china.org.cn/english/2003/Jul/69295.htm>
- 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. (2004). New York: Norton. Retrieved 7/20/09 from <http://www.9-11commission.gov/report/911Report.pdf>
- 2,000 sign up for enhanced driver's license. (2008). Retrieved 5/20/09, from <http://www.rfidnews.org/2008/01/24/2000-sign-up-for-enhanced-drivers-license>
- A closer look at the FBI's joint terrorism task forces. (2004). Retrieved 7/20, 2009, from <http://www.fbi.gov/page2/dec04/jttf120114.htm>
- ADB country partnership strategy: People's Republic of China 2008-10. (2008, February). Asian Development Bank. Retrieved May 1, 2009 from <http://www.adb.org/Documents/CPSs/PRC/2008/CPS-PRC-2008-2010.pdf>.
- Aftergood, S. (2008, July 30). A reorganization of defense intelligence. *Secrecy News*. Retrieved 5/1/2009 from [http://www.fas.org/blog/secrecy/2008/07/defense\\_intel\\_reorg.html](http://www.fas.org/blog/secrecy/2008/07/defense_intel_reorg.html)
- Agre, P., & Rotenberg, M. (1997). *Technology and privacy: The new landscape*. Cambridge, Mass.: MIT Press.
- Airline reservation system and passenger name record (PNR) access by states. (2004, March 15). International Air Travelers' Association (IATA). No. FAL/12-WP/74).
- Akdeniz, Y. (2002). Anonymity, democracy, and cyberspace. *Social Research*, 69(11), 223-237.

- Albrecht, K. (2008). *Testifying against REAL ID and enhanced driver's licenses in Arizona*. Retrieved 5/19/2009, 2009, from [http://www.spsychips.com/blog/2008/03/testifying\\_against\\_real\\_id\\_and.html](http://www.spsychips.com/blog/2008/03/testifying_against_real_id_and.html)
- Allen, A. L. (2003). Theory and practice of accountability. *Why privacy isn't everything: Feminist reflections on personal accountability* (pp. vii, 211 p.-1). Lanham, Md.: Rowman & Littlefield.
- Allen, A.L. (1996). Constitutional law and privacy. In D. M. Patterson (Ed.). *A companion to philosophy of law and legal theory* (pp. 139-155). Cambridge, Mass.: Blackwell Publishers.
- Alonzo, M. (2004). Flaming in electronic communication. *Decision Support Systems*, 36(3), 205.
- Altman, I. (1981). The environment and social behavior: Privacy, personal space, territory, crowding (1st Irvington ed.). New York, N.Y.: Irving Publishers.
- Aly, G., Roth, K. H., Black, E., & Oksiloff, A. (2004). *The Nazi census: Identification and control in the third reich* [Restlose Erfassung.] . Philadelphia: Temple University Press.
- Amazon.com: What are statistically improbable phrases? Retrieved 3/11/2009, 2009, from <http://www.amazon.com/gp/search-inside/sipshelp.html>
- Anderson, C. (2005, Jan 13). FBI computer overhaul hits another snag. *AP*.
- Andrejevic, M. (2007). *iSpy: Surveillance and power in the interactive era*. Lawrence, Kan.: University Press of Kansas.
- Angle, S.C. (1998). Did someone say "rights"? Liu Shipei's concept of quanli. *Philosophy East and West*, 48(4), 623-651.
- Angle, S.C. (2002). *Human rights and Chinese thought: A cross-cultural inquiry*. Cambridge; New York: Cambridge University Press.
- Arendt, H. (1951). *The origins of totalitarianism* (1st ed.). New York: Harcourt, Brace.

- Automating apartheid: U.S. computer exports to South Africa and the arms embargo. (1982). National Action/Research on the Military-Industrial Complex, & American Friends Service Committee. Philadelphia: NARMIC/America Friends Service Committee.
- Austin, J.L. (1962). *How to do things with words*. Oxford: Clarendon Press.
- Baidu accused of violating user privacy*. (March 13, 2007). Retrieved March 15, 2008, from <http://www.chinatechnews.com/2007/03/13/5089-baidu-accused-of-violating-user-privacy/>
- Baker, C.E. (2004). Autonomy and informational privacy, or gossip: The central meaning of the first amendment. *Social Philosophy & Public Policy*, 21, 215.
- Baker, S. A. (2008). *Setting the record straight on REAL ID (part III) – too much spaghetti*. Retrieved 5/19/2009 from [http://www.dhs.gov/journal/leadership/2008/03/setting-record-straight-on-real-id-part\\_28.html#comments](http://www.dhs.gov/journal/leadership/2008/03/setting-record-straight-on-real-id-part_28.html#comments)
- Bakken, B. (2000). The exemplary society: Human improvement, social control, and the dangers of modernity in China. Oxford England New York: Oxford University Press.
- Ball, K., & Haggerty, K. D. (2005). Editorial: Doing surveillance studies. *Surveillance & Society*, 3(2/3), 129-138.
- Ball, K., & Webster, F. (2003). The intensification of surveillance: Crime, terrorism and warfare in the information age (1st ed.). London ; Sterling, Va.: Pluto Press.
- Balkin, J. (2003). The proliferation of legal truth. *Harvard Journal of Law & Public Policy*, 26 (Winter), 5.
- Bambauer, D. (2006). Cool tools for tyrants. *Legal Affairs*, (January-February).
- Barbaro, M., & Zeller, T.J. (2006, August 9). A face is exposed for AOL searcher no. 4417749. [Electronic version]. *New York Times*, Retrieved May 1, 2008 from [http://www.nytimes.com/2006/08/09/technology/09aol.html?\\_r=1&ex=1312776000&pagewanted=print&oref=slogin](http://www.nytimes.com/2006/08/09/technology/09aol.html?_r=1&ex=1312776000&pagewanted=print&oref=slogin)

- Batson, A. (2003, August 12). China begins effort to replace citizen IDs with digital cards. *Wall Street Journal*.
- Beck, U. (1999). *World risk society*. Cambridge, UK ; Malden, Mass: Polity Press.
- Bennett, C. (2008a). Unsafe at any altitude: The comparative politics of no-fly lists in the united states and canada. In M. B. Salter (Ed.), *Politics at the airport* (pp. 51-76). Minneapolis: University of Minnesota Press.
- Bennett, C. J. (2008b). *The privacy advocates: Resisting the spread of surveillance*. Cambridge, MA: MIT Press.
- Beniger, J. R. (1986). *The control revolution: Technological and economic origins of the information society*. Cambridge, Mass.: Harvard University Press.
- Berghel, H. (2000). Identity theft, social security numbers, and the web. *Communications of the ACM*, 43(2), 17-21.
- Berton, J. (2006). Gen Y not shy sharing online — but worries about spying. *San Francisco Chronicle*, September 15, 2007.
- Berger, P. L., & Luckmann, T. (1966). *The social construction of reality; a treatise in the sociology of knowledge* ([1st ed.]). Garden City, N.Y.: Doubleday.
- Best, S.J., Krueger, B.S., & Ladewig, J. (2006). The polls — trends: Privacy in the information age. *Public Opinion Quarterly*, 70(3), 375-401.
- Bloggers should get real in virtual world. (2006). Retrieved 5/9/2009, from [http://english.people.com.cn/200612/13/eng20061213\\_331956.html](http://english.people.com.cn/200612/13/eng20061213_331956.html)
- Blumenthal, P. (2009). Congress had no time to read the USA PATRIOT act. Retrieved 5/1, 2009, from <http://blog.sunlightfoundation.com/2009/03/02/congress-had-no-time-to-read-the-usa-patriot-act/>
- Bradley, J. (1984, May 7). China to Issue National ID Cards. *AP*.
- Bradsher, K. (2007a, September 11). An opportunity for Wall Street in China's surveillance boom. *The New York Times*, pp. 1.

- Bradsher, K. (2007b, August 12). China enacting high - tech plan to track people. *The New York Times*, pp. 1.
- Bratton, W.J. (2008, March). National fusion center conference speech. San Francisco, CA.  
Retrieved 7/20/09 from [http://www.cpt-mi.org/pdf/Fusion\\_Center\\_Speech\\_3-14-08.pdf](http://www.cpt-mi.org/pdf/Fusion_Center_Speech_3-14-08.pdf)
- Braudel, F. (1980). *On history* (S. Matthews Trans.). Chicago: University of Chicago Press.
- Broache, A. (2008). DHS: Real ID could help shut down meth labs. Retrieved 5/19/ 2009, from [http://news.cnet.com/8301-10784\\_3-9851813-7.html](http://news.cnet.com/8301-10784_3-9851813-7.html)
- Brubaker, R. (1984). *The limits of rationality: An essay on the social and moral thought of Max Weber*. London; Boston: Allen & Unwin.
- Bruce, L. (2006). *Suspicious activity reports (SARs): U.S. bank program may create secret report on you*. Retrieved 2/26/2009, from <http://www.bankrate.com/cbsmw/news/bank/20060628a1.asp>
- Burns, R. (2007, August 21). Pentagon to suspend anti-terror database. [Electronic version]. *USA Today*. Retrieved 7/24/2009 from [http://www.usatoday.com/news/washington/2007-08-21-3764146505\\_x.htm](http://www.usatoday.com/news/washington/2007-08-21-3764146505_x.htm)
- CAGW: REAL ID regulations omit the worst. (2007). Retrieved 6/13/ 2009, from <http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=109&STORY=/www/story/03-01-2007/0004537961&EDATE=>
- Calvin, M. (2007, May 1). Re: Docket # DHS-2006-0030 minimum standards for Driver's licenses and identification cards acceptable by federal agencies for federal purposes (Official letter from American Association of Motor Vehicle Administrators (AAMVA) to DHS). Retrieved 7/10/09 from <http://www.aamva.org/aamva/DocumentDisplay.aspx?id={A355DF44-2049-41AB-9961-2C1C73F7E707}>.
- Capurro, R. (2006). Towards an ontological foundation of information ethics. *Ethics and Information Technology*, 8(4), 175-186.

- Cao, J. (2005). Protecting the right to privacy in China. *Victoria University of Wellington Law Review*, 36(3), 645-664.
- Caterinicchia, D. (2006, October 18). Privacy group files suit against FBI over disclosure of investigative data-base records. [Electronic version]. *AP*, from Lexis-Nexis database.
- Chang, N. (2002). *Silencing political dissent* (1st ed.). New York: Seven Stories Press.
- Changsha Intermediate People's Court of Hunan Province criminal verdict, Changsha Intermediate Criminal Division One First Trial Case No. 29 (2005). Retrieved 5/12/09 from [http://lawprofessors.typepad.com/china\\_law\\_prof\\_blog/files/ShiTao\\_verdict.pdf](http://lawprofessors.typepad.com/china_law_prof_blog/files/ShiTao_verdict.pdf)
- Chao, L. (2009, March 5). Lenovo looks to grow in rural China. [Electronic version]. *The Wall Street Journal*, Retrieved March 30, 2009 from <http://online.wsj.com/article/SB123617998640930287.html>
- Checkland, P. (1981). *Systems thinking, systems practice*. Chichester Sussex; New York: J. Wiley.
- Chen, F. (2007, May 22). China eases off proposal for real-name registration of bloggers. [Electronic version]. *Xinhua*, Retrieved September 23, 2007 from [http://news.xinhuanet.com/english/2007-05/22/content\\_6136185.htm](http://news.xinhuanet.com/english/2007-05/22/content_6136185.htm)
- Chen, J. (2004). *Popular political support in urban China*. Washington, D.C.; Stanford, Calif.: Woodrow Wilson Center Press; Stanford University Press.
- China leads the U.S. in digital self expression (2007). Retrieved March 23, 2008, from [http://www.iac.com/index/news/press/IAC/press\\_release\\_detail.htm?id=8833](http://www.iac.com/index/news/press/IAC/press_release_detail.htm?id=8833)
- China provides access to ID database to curb fraud (2007). Retrieved March 1, 2008, from [http://news.xinhuanet.com/english/2007-02/09/content\\_5720728.htm](http://news.xinhuanet.com/english/2007-02/09/content_5720728.htm)
- China's public security and surveillance network the golden shield project now connects over 800,000 computers according to state media (2007, March 2). *China IT & Telecom Report*.

- China public security technology wins Shenzhen card system contract.(2007, July 30). [Electronic version]. *Computer Business Review*. Retrieved 9/5/08 from [http://www.cbronline.com/article\\_news.asp?guid=1DD78558-187D-41E](http://www.cbronline.com/article_news.asp?guid=1DD78558-187D-41E)
- China starts working out law on citizen ID card. (2002, October 31). *People's Daily*.
- China tightens rules for online chat rooms. (2005). Retrieved 5/10/2009 from [http://www.upi.com/Top\\_News/2005/03/18/China-tightens-rules-for-online-chat-rooms/UPI-18261111147137/](http://www.upi.com/Top_News/2005/03/18/China-tightens-rules-for-online-chat-rooms/UPI-18261111147137/)
- China to pour U.S.\$120 billion into information industry. (2001). Retrieved 5/8/2009 from [http://www.china.org.cn/archive/2001-09/30/content\\_1019921.htm](http://www.china.org.cn/archive/2001-09/30/content_1019921.htm)
- China to set up database on pyramid-scheme dealers to step up crackdown. (2006, September 21). *Xinhua*.
- China to set up national database of suspected drug traffickers. (2005, August 11). *Xinhua*.
- Chow, K. W. (1993). The politics of performance appraisal. In M. K. Mills, & S. S. Nagel (Eds.), *Public administration in China* (pp. 105-122). Westport, Conn.: Greenwood Press.
- Church, F., (1976). Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities. United States Senate, 94th Congress, 2nd Session, April 26 (legislative day, April 14), 1976. [AKA "Church Committee Report"]. Archived on COINTELPRO sources website, retrieved 3/7/09 from <http://www.icdc.com/~paulwolf/cointelpro/cointel.htm>
- Clarke, R. (1994). Dataveillance by governments: The technique of computer matching. *Information Technology & People*, 7(2), 46-85.
- Cohen, J. E. (2003). Overcoming property: (does copyright trump privacy?). *University of Illinois Journal of Law, Technology & Policy*, 101-108.
- Cohen, J. E. (2000). Examined lives: Informational privacy and the subject as object. *Stanford Law Review*, 52, 1373.

- Collins, D. (2003, September 25). Pentagon Terror Spy Lab Closed. Retrieved 7/20/09 from <http://www.cbsnews.com/stories/2003/07/31/attack/main566133.shtml>
- Collings, R.B. (2005, Oct.25). In re Application of the United States of America for an Order Authorizing the Use of a Pen Register and Trap on [xxx] Internet Service Account/ User Name [xxxxxxxx@xxx.com], Nos. 2005M0499RBC, 2005MO500RBC, 2005MO501RBC, 2005MO502RBC. U.S. District Court for the District of Massachusetts.
- Connecting the dots using new FBI technology (2008). Retrieved 5/20/ 2009, from [http://www.fbi.gov/page2/sept08/eguardian\\_091908.html](http://www.fbi.gov/page2/sept08/eguardian_091908.html)
- Confirm a friend, catch a crook, or betray your neighbors: China's surveillance state goes mobile (2006). Retrieved May 1, 2008, from [http://angrychineseblogger.blog-city.com/confirm\\_a\\_friend\\_catch\\_a\\_crook\\_or\\_betray\\_your\\_neighbors\\_chin.htm](http://angrychineseblogger.blog-city.com/confirm_a_friend_catch_a_crook_or_betray_your_neighbors_chin.htm)
- Cope, S. (2007). *REAL ID creeps into the immigration debate*. Retrieved 5/19/ 2009, from <http://blog.cdt.org/2007/06/05/real-id-creeps-into-the-immigration-debate/>
- Court rejects students' kiss video lawsuit. (2004, August 24). [Electronic version]. *China Daily*. Retrieved May 12, 2008 from [http://www.chinadaily.com.cn/english/doc/2004-08/24/content\\_368327.htm](http://www.chinadaily.com.cn/english/doc/2004-08/24/content_368327.htm)
- Crampton, T. (2006, March 20). Innovation may lower net users' privacy. [Electronic version]. *International Herald Tribune*. Retrieved January 10, 2008 from <http://www.iht.com/articles/2006/03/19/business/chinet20.php>
- Dandeker, C. (1990). *Surveillance, power, and modernity: Bureaucracy and discipline from 1700 to the present day*. New York: St. Martin's Press.
- Davis, J. K. (1992). *Spying on America: The FBI's domestic counterintelligence program*. New York: Praeger.
- DeCew, J. W. (1997). In pursuit of privacy: Law, ethics, and the rise of technology. Ithaca: Cornell University Press.



- DefenseLink news release: DoD to implement interim threat reporting procedures. (2007).  
Retrieved 6/18/2009, from  
<http://www.defenselink.mil/releases/release.aspx?releaseid=11251>
- Deignan, A. (2005). *Metaphor and corpus linguistics*. Amsterdam; Philadelphia: J. Benjamins Pub.
- Derlega, V. J., & Chaikin, A. L. (1975). *Sharing intimacy: What we reveal to others and why*. Englewood Cliffs, N.J.: Prentice-Hall.
- DHS: Remarks by Secretary Chertoff at a press conference on REAL ID. (2007). Retrieved 5/20/2009, 2009, from [http://www.dhs.gov/xnews/releases/pr\\_1172834392961.shtm](http://www.dhs.gov/xnews/releases/pr_1172834392961.shtm)
- Dibble, V. K. (1963). Four types of inference from documents to events. *History and Theory*, 3(2), 203-221.
- Dickie, M. (2007, July 8). China city to tighten internet controls. [Electronic version]. *Financial Times* (London, England), Retrieved March 1, 2008 from  
[http://www.ft.com/cms/s/0/0790fcb6-2d7c-11dc-939b-0000779fd2ac.html?ncklick\\_check=1](http://www.ft.com/cms/s/0/0790fcb6-2d7c-11dc-939b-0000779fd2ac.html?ncklick_check=1)
- Dogan, M., & Pélassy, D. (1990). *How to compare nations: Strategies in comparative politics* [Sociologie politique comparative.] (2nd ed.). Chatham, N.J.: Chatham House.
- Donohue, L. K. (2006). Anglo-American privacy and surveillance. *Journal of Criminal Law & Criminology*, 96(3), 1059-1208.
- Donner, F. J. (1981; 1980). *The age of surveillance: The aims and methods of America's political intelligence system* (1st Vintage Books ed.). New York: Vintage Books.
- Duncan, G. T. (2003). Exploring the tension between privacy and the social benefits of governmental databases. Paper Presented at *Security, Technology, and Privacy: Shaping a 21st Century Public Information Policy*, April 24-25, Georgetown University Law Center, Washington, DC.
- Dutton, M. R. (2005). *Policing Chinese politics: A history*. Durham: Duke University Press.

- Dutton, M. R. (1992). *Policing and punishment in China: From patriarchy to "the people"*. Cambridge; New York: Cambridge University Press.
- Dubose, L. (1987, May 15). The next round-up. *The Texas Observer*, n.p.
- Eaton, J. W. (1986). *Card-carrying Americans: Privacy, security, and the national ID card debate*. Totowa, N.J.: Rowman & Littlefield.
- Einhorn, B., Elgin, B., & Burrows, P. (2006, September 18). Helping big brother go high tech; Cisco, Oracle, and other U.S. companies are supplying china's police with software and gear that can be used to keep tabs on criminals and dissidents. *Business Week*, 46.
- EPIC comments on the TSA aviation security screening records privacy act notice (2003). Retrieved 6/12/2009 from <http://epic.org/privacy/airtravel/tsacomment2.24.2003.html>
- Entman, R. M. (1993). Framing: Toward clarification of a fractured paradigm. *Journal of Communication*, 43(4), 51-58.
- Ericson, R. V., & Haggerty, K. D. (1997). *Policing the risk society*. Toronto; Buffalo: University of Toronto Press.
- Etzioni, A. (1999). *The limits of privacy*. New York: Basic Books.
- Etzioni, A. (1988). Political power and intra-market structures. *The moral dimension* (pp. 217-236) Free Press.
- Fact sheet: Enhanced driver's licenses (EDL) (2007). Retrieved 2/22, 2009 from [http://www.dhs.gov/xnews/releases/pr\\_1196872524298.shtm](http://www.dhs.gov/xnews/releases/pr_1196872524298.shtm)
- Fewsmith, J. (2007). Assessing social stability on the eve of the 17th party congress. *China Leadership Monitor*, 20, 1-24.
- Finley, B. (2008, June 29). Terror watch uses local eyes 181. [Electronic version]. *Denver Post*, Retrieved 3/23/09 from [http://www.denverpost.com/news/ci\\_9725077](http://www.denverpost.com/news/ci_9725077)
- Fisher, K. (2007). Microsoft sued over WGA spyware allegations in China. Retrieved 2/5, 2008 from <http://arstechnica.com/news.ars/post/20070916-microsoft-sued-over-wga-spyware-allegations-in-China.html>

- Fleck, L. (1979). *Genesis and development of a scientific fact*. Chicago: University of Chicago Press.
- Foucault, M. (1985). In Pearson J. (Ed.), *Discourse and truth: The problematization of parrhesia*. Evanston, Illinois: Northwestern University. Retrieved 7/20/2009 from <http://foucault.info/documents/parrhesia/>
- Foucault, M. (1979). *Discipline and punish: The birth of the prison*. New York: Vintage Books.
- Foucault, M. (1972). *The archaeology of knowledge; and, the discourse on language*. New York: Pantheon Books.
- Fried, C. (1968). Privacy. *The Yale Law Journal*, 77(3), 475-493.
- Froomkin, M. (2002). Uneasy case for national ID cards as a means to enhance privacy. Paper presented at *the 30th Annual Telecommunications Policy Research Conference*, Washington, D.C. Retrieved 7/1/2009 from <http://osaka.law.miami.edu/~froomkin/articles/ID1.pdf>
- Furth, C. (2002). Solitude, silence and concealment: Boundaries of the social body in Ming dynasty China. In B. S. McDougall, & A. Hansson (Eds.), *Chinese concepts of privacy* (pp. 274-53). Leiden; Boston; Koln: Brill.
- Fussell, J. (2004). Genocide and group classification on ID cards. In C. Watner, & W. McElroy (Eds.), *National identification systems: Essays in opposition* (pp. 55-69). Jefferson, N.C.: McFarland & Co.
- Gallagher, R. (2007, May 10). Could you be on the FBI's terrorist watch list? [Electronic version]. *Medill Reports*, Retrieved 2/12/2009 from <http://news.medill.northwestern.edu/chicago/news.aspx?id=36117&print=1>
- Gandy, O.H. (2003). Public opinion surveys and the formation of privacy policy. *Journal of Social Issues*, 59(2), 283-299.
- Gandy Jr., O. H. (2000). Audience construction: Race, ethnicity and segmentation in popular media. *50th Annual Conference of the International Communication Association*.

- Gandy Jr., O. H. (1995). It's discrimination stupid! In J. Brook, & I. A. Boal (Eds.), *Resisting the virtual life: The culture and politics of information* (pp. 35-48). San Francisco; Monroe, OR: City Lights; Subterranean Co. distributor.
- Gandy Jr., O. H. (1993). *The panoptic sort: A political economy of personal information*. Boulder, Colo.: Westview.
- Gandy Jr., O. H. (1982). *Beyond agenda setting: Information subsidies and public policy*. Norwood, N.J.: Ablex Pub. Co.
- Gantz, J. F., Chute, C., Manfrediz, A., Minton, S., Reinsel, D., & Schlichting, W., (2008). *The diverse and exploding digital universe*. IDC. Retrieved 3/12/09 from <http://www.emc.com/collateral/analyst-reports/diverse-exploding-digital-universe.pdf>
- Garfinkel, S., Juels, A., & Pappu, R. (2005). RFID privacy: An overview of problems and proposed solutions. *IEEE Security & Privacy*, 3(3), 34-43.
- Gavison, R. (1980). Privacy and the limits of the law. *Yale Law Journal*, 89(3), 421-471.
- Geiger, H. (2008). IG: Terror database filled with outdated, unfounded information. Retrieved 7/12, 2009 from <http://blog.cdt.org/2008/11/19/ig-fbi-terror-database-riddled-with-incomplete-out-of-date-and-baseless-threat-records/>
- Gellman, B. (2005, November 6). The FBI's secret scrutiny; in hunt for terrorists, bureau examines records of ordinary Americans. *The Washington Post*.
- Gellman, R. (1997). Does privacy law work? In P. Agre, & M. Rotenberg (Eds.), *Technology and privacy: The new landscape* (pp. 193-218). Cambridge, Mass.: MIT Press.
- Giddens, A. (1985). *A contemporary critique of historical materialism. vol.2, the nation-state and violence*. London: Polity.
- Gilliom, J. (2001). *Overseers of the poor: Surveillance, resistance, and the limits of privacy*. Chicago: University of Chicago Press.
- Gillis, A. R. (1989). Crime and state surveillance in nineteenth-century France. *The American Journal of Sociology*, 95(2), 307-341.

- Gilmore, G. J. (2005, December 15). DoD orders review of anti-threat intel-gathering system. *American Forces Press Service*.
- Goldsmith, J. L. (2007). *The terror presidency: Law and judgment inside the Bush administration* (1st ed.). New York: W.W. Norton.
- Goldstein, R. J. (2001). *Political repression in modern America from 1870 to 1976* (1 Illinois ed.). Urbana: University of Illinois Press.
- Golinski, J. (2005). *Making natural knowledge: Constructivism and the history of science*. Chicago: University of Chicago Press.
- Google - Yahoo market battle threatens freedom of expression (2004, July 26). Retrieved 5/12/09 from <http://www.rsf.org/Google-Yahoo-market-battle.html>.
- Gorham-Oscilowski, U., & Jaeger, P. T. (2008). National security letters, the USA PATRIOT act, and the constitution: The tensions between national security and civil rights. *Government Information Quarterly*, 25, 625-644.
- Gorman, S. (2008, November 25). In cities, the fight against terrorism walks the beat. [Electronic version]. *Wall Street Journal*. Retrieved February 12, 2009 from <http://sec.online.wsj.com/article/SB122757233321954813.html>
- Government secretly tracks millions of Americans. (2006). Retrieved 6/12/2009 from [http://www.aclunc.org/news/press\\_releases/government\\_secretly\\_tracks\\_millions\\_of\\_americans.shtml](http://www.aclunc.org/news/press_releases/government_secretly_tracks_millions_of_americans.shtml)
- Greenwald, G. (2009, April 6). New and worse secrecy and immunity claims from the Obama DOJ. [Electronic version]. *Salon Magazine*. Retrieved 6/22/09 from <http://www.salon.com/opinion/greenwald/2009/04/06/obama/>
- Gross, G. (2005, October 26). United States to require RFID chips in passports. [Electronic version]. Retrieved 6/8/2009 [http://www.pcworld.com/article/123246/united\\_states\\_to\\_require\\_rfid\\_chips\\_in\\_passports.html](http://www.pcworld.com/article/123246/united_states_to_require_rfid_chips_in_passports.html)

Guo, L. (2006). Under the "golden shine": China's efforts to bridge government and citizens.

*Regional Development Dialogue*, 27(2), 20.

Gutmann, E. (2004). *Losing the new China: A story of American commerce, desire, and betrayal*

(1st ed.). San Francisco: Encounter Books.

Habermas, J. (1989). *The structural transformation of the public sphere: An inquiry into a*

*category of bourgeois society [Strukturwandel der Öffentlichkeit]*. Cambridge, Mass.:

MIT Press.

Hargrove, T. (2006). *Third of Americans suspect 9-11 government conspiracy*. Retrieved May 12,

2008, from <http://www.scrippsnews.com/911poll>

Harris, D. (2007). China's law enforcement rising. *China Law Blog*, September 20, 2007.

Retrieved March 10, 2008, from

[http://www.chinalawblog.com/2007/09/whither\\_the\\_china\\_visa.html](http://www.chinalawblog.com/2007/09/whither_the_china_visa.html)

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of*

*Sociology*, 51(4), 605-622.

Hallin, D. C., & Mancini, P. (2004). *Comparing media systems: Three models of media and*

*politics*. Cambridge, UK; New York, NY: Cambridge University Press.

Harris, S. (2006, February 23, 2006). TIA lives on. [Electronic version]. *National Journal*.

Retrieved November 1, 2007 from

<http://nationaljournal.com/about/njweekly/stories/2006/0223nj1.htm>

Hasbrouck, E. (2003). Consolidated comments of Edward Hasbrouck re: Establishment and

exemption from the privacy act of records system DOT/TSA 010, "Aviation security-screening records (ASSR)". Retrieved 1/27, 2009, from

[http://www.hasbrouck.org/articles/Hasbrouck\\_TSA\\_comments-30SEP2003.pdf](http://www.hasbrouck.org/articles/Hasbrouck_TSA_comments-30SEP2003.pdf)

Hasbrouck, E. (2004). *What's wrong with CAPPS-II?* Retrieved 1/13, 2009, from

<http://www.hasbrouck.org/articles/CAPPS-II.html>

- Hays, C. L. (2004, November 14). What Wal-mart knows about customers' habits. [Electronic version]. *New York Times*. Retrieved May 1, 2008 from <http://www.nytimes.com/2004/11/14/business/yourmoney/14wal.html>
- Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology*, 51(4), 605-622.
- Hanlon, M. (2008). *The tipping point: One in two humans now carries a mobile phone*. Retrieved 5/8/2008 from <http://www.gizmag.com/mobile-phone-penetration/8831/>
- Henkin, L. (1974). Privacy and autonomy. *Columbia Law Review*, 74, 1410-33.
- Hertz, E. (2001). Face in the crowd: The cultural construction of anonymity in urban China. In N. Chen, C. D. Clark, S. Z. Gottschang & L. Jeffery (Eds.), *China urban: Ethnographies of contemporary culture* (pp. 274). Durham; London: Duke University Press.
- Heyman, D. (2008). Finding the Enemy Within: Towards a Framework for Domestic Intelligence, in Bert B. Tussing, ed., *Threats at Our Threshold: Homeland Defense and Homeland Security in the New Century*, Washington, D.C.: Center for Strategic and International Studies, 2000, pp. 149 –174. Retrieved 7/13/09 from [http://csis.org/images/stories/HomelandSecurity/071022\\_Chap4-FindingTheEnemyWithin.pdf](http://csis.org/images/stories/HomelandSecurity/071022_Chap4-FindingTheEnemyWithin.pdf)
- Hine, C. (2000). *Virtual ethnography*. London ; Thousand Oaks, Calif.: Sage.
- Holquist, P. (1997). "Information is the alpha and omega of our work": Bolshevik surveillance in its pan-european context. *The Journal of Modern History*, 69(3), 415-450.
- Homeland security appropriations bill purports to restrict use of funds for CAPPS II. (2003, October 1). Retrieved 8/1, 2008 from <http://www.techlawjournal.com/topstories/2003/20031001.asp>
- Hudson, A. (2009, February 20). Napolitano debates real ID. *Washington Times*, n.p.
- Human rights achievements in China. (2000). Retrieved 3/12, 2008, from <http://www.china-embassy.org/eng/zt/zgrq/t36636.htm>

- Hunter, R. (2002). *World without secrets: Business, crime, and privacy in the age of ubiquitous computing*. New York: J. Wiley.
- Hutchby, I. (2001). Technologies, texts and affordances. *Sociology-the Journal of the British Sociological Association*, 35(2), 441-456.
- Identification: Ministries seek to tighten ID system (BBC summary translation). (1993, January 5). *New China News*.
- IFPI: 07 digital music report (2007). International Federation of the Phonographic Industry.  
Retrieved 6/22/09 from <http://www.ifpi.org/content/library/digital-music-report-2007.pdf>
- InfraGard: FBI and private sector join to safeguard critical infrastructures. (2004). Retrieved 6/30/09, 2009 from <http://www.fbi.gov/page2/dec04/infragard121404.htm>
- Interagency threat assessment and coordination group. Retrieved 8/26, 2009, from <http://www.ise.gov/pages/partner-itacg.html>
- International Campaign against Mass Surveillance (ICAMS). (2005, April). *The emergence of a global infrastructure for mass registration and surveillance*. Retrieved 7/20/2009 from <http://i-cams.org/ICAMS1.pdf>.
- Internet database tracks criminals. (2005, November 17). [Electronic version]. *China Daily*.  
Retrieved 8/23/08 from <http://www.china.org.cn/english/Life/149044.htm>
- Isikoff, M. (2006, January 30). The other big brother. [Electronic version]. *Newsweek*, Retrieved 6/18/2009 from <http://www.newsweek.com/id/47425>
- Jensen, D., Rattigan, M., & Blau, H. (2003). Information awareness: A prospective technical assessment. Paper presented at the *Proceedings of the Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Washington, D.C. 378-387.  
Retrieved 7/1/08 from [http://portal.acm.org/ft\\_gateway.cfm?id=956794&type=pdf&coll=GUIDE&dl=GUIDE&CFID=46861063&CFTOKEN=83201743](http://portal.acm.org/ft_gateway.cfm?id=956794&type=pdf&coll=GUIDE&dl=GUIDE&CFID=46861063&CFTOKEN=83201743)



- Jiang, M. (2008). *China Unicom sued for advertising oil and wine*. Retrieved May 7, 2008 from [http://www.pacificepoch.com/newsstories/122827\\_0\\_5\\_0\\_M/](http://www.pacificepoch.com/newsstories/122827_0_5_0_M/)
- Johnson, K. (2004, December 1). Anti-terrorism methods draw ACLU scrutiny. Retrieved 7/20/09 from [http://www.usatoday.com/news/washington/2004-12-01-aclu-anti-terror\\_x.htm](http://www.usatoday.com/news/washington/2004-12-01-aclu-anti-terror_x.htm)
- Jonas, J. & J. Harper (2006, December 11). Effective Counterterrorism and the Limited Role of Predictive Data Mining. Retrieved July 28, 2009, from *The Cato Institute* web site: [http://www.cato.org/pub\\_display.php?pub\\_id=6784](http://www.cato.org/pub_display.php?pub_id=6784)
- Jones, T. (2009). In warrantless wiretapping case, Obama DOJ's new arguments are worse than Bush's. Retrieved 6/12, 2009, from <http://www.eff.org/deeplinks/2009/04/obama-doj-worse-than-bush>
- Kalathil, S., & Boas, T. C. (2003). *Open networks, closed regimes: The impact of the internet on authoritarian rule*. Washington, D.C.: Carnegie Endowment for International Peace.
- Kassof, A. (1964). The administered society: Totalitarianism without terror. *World Politics*, 16(4), 558-575.
- Ke, H. (2005). .Cn. In S. Y. Chin (Ed.), *Digital review of Asia pacific 2005/2006* (pp. 89-95). Penang: Southbound.
- Keane, M. (2005). China's national resident identity card. *UCLA Pacific Basin Law Journal*, 23(1), 212-242.
- Kent, S. T., & Millett, L. I. (2003). *Who goes there? Authentication through the lens of privacy*. Washington, D.C.: National Research Council, Committee on Authentication Technologies and Their Privacy Implications. National Academies Press.
- Kerr, O. S. (2003). Internet surveillance law after the USA patriot act: The big brother that isn't. *Northwestern University Law Review*, 97(2), 607-673.

- Kissing couple to sue metro over video. (2008, January 22). [Electronic version]. *China Daily*. Retrieved April 10, 2008 from [http://www.chinadaily.com.cn/China/2008-01/22/content\\_6412351.htm](http://www.chinadaily.com.cn/China/2008-01/22/content_6412351.htm)
- Klein, N. (2008, May 29). China's all-seeing eye. [Electronic version]. *Rolling Stone*. Retrieved 11/24/2009 from [http://www.rollingstone.com/politics/story/20797485/chinas\\_allseeing\\_eye/print](http://www.rollingstone.com/politics/story/20797485/chinas_allseeing_eye/print)
- Kluegel, J. R., Mason, D. S., & Wegener, B. (1995). *Social justice and political change: Public opinion in capitalist and post-communist states*. New York: A. de Gruyter.
- Kluver, R. (2005). The architecture of control: A Chinese strategy for e-governance. *Journal of Public Policy*, 25(1), 75-97.
- Knoke, D. (2004). The sociopolitical construction of national policy domains. In C. H. C. A. Henning, & C. Melbeck (Eds.), *Interdisziplinäre sozialforschung: Theorie und empirische anwendungen* (pp. 81-15). Frankfurt: Capus Verlag.
- Ko, J. W. (2004). Comment: The fourth amendment and the wiretap act fail to protect against random ISP monitoring of E-mails for the purpose of assisting law enforcement. *John Marshall Journal of Computer & Information Law*, 22(2), 493.
- Kohn, J. The Hannah Arendt papers: Totalitarianism: The inversion of politics. Retrieved 3/30/2009, 2009, from <http://lcweb2.loc.gov/ammem/arendthtml/essayb1.html>
- Kohn, M. L. (1987). Cross-national research as an analytic strategy: American sociological association, 1987 presidential address. *American Sociological Review*, 52(6), 713.
- Krippendorff, K. (1996). A second-order cybernetics of otherness. *Systems Research*, 13(3), 311-328.
- Krippendorff, K. (1993). Major metaphors of communication and some constructivist reflections on their use. *Cybernetics & Human Knowing*, 2(1), 3-25; 3.
- Lakoff, G., & Johnson, M. (1980). *Metaphors we live by*. Chicago: University of Chicago Press.

- Latour, B., & Woolgar, S. (1986; 1979). *Laboratory life: The construction of scientific facts*. Princeton, N.J.: Princeton University Press.
- Laudon, K. C. (1986). *Dossier society: Value choices in the design of national information systems*. New York: Columbia University Press.
- Lawmakers hail protection of civil rights under China's new ID card law (2003, July 2). *BBC Monitoring International Reports*.
- Leahy, P. (2006, December 6). FBI oversight: Hearings before the Judiciary Committee, U.S. Senate Testimony. Retrieved 3/23/08, from [http://judiciary.senate.gov/hearings/testimony.cfm?id=2453&wit\\_id=2629](http://judiciary.senate.gov/hearings/testimony.cfm?id=2453&wit_id=2629)
- Lear, R. S., & Reynolds, J. D. (2003). Your social security number or your life: Disclosure of personal identification information by military personnel and the compromise of privacy and national security. *Boston University International Law Journal*, 21(1), 1-28.
- Lee, H. Y. (1990). *From revolutionary cadres to party technocrats in socialist China*. Berkeley: University of California Press.
- Lemon, S. (2006, March 9). China to issue 1.3 billion RFID identification cards. [Electronic version]. *IDG News Service*. Retrieved 3/24/2009, from [http://www.computerworld.com/s/article/109360/China\\_to\\_issue\\_1.3\\_billion\\_RFID\\_identification\\_cards?taxonomyId=084](http://www.computerworld.com/s/article/109360/China_to_issue_1.3_billion_RFID_identification_cards?taxonomyId=084)
- Lemos, R. (2006). *Experts: National ID won't solve terrorism*. Retrieved 7/23/2009, 2009, from <http://www.securityfocus.com/brief/144>
- Li, L. (2004). Political trust in rural China. *Modern China*, 30(2), 228-258.
- Lilie, C. (2004, October). Multiforce protection in a portal - SIGNAL magazine. [Electronic version]. *SIGNAL*. Retrieved 6/18/2009 from [http://www.afcea.org/signal/articles/templates/SIGNAL\\_Article\\_Template.asp?articleid=418&zoneid=3](http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=418&zoneid=3)

- Lindorff, D. (2002, August 30). New life for operation TIPS. [Electronic version]. *Salon.com*, Retrieved 4/23/08 from <http://archive.salon.com/news/feature/2002/08/30/tips/print.html>
- Lipowicz, A. (2007, February 12). DHS tunes out RFID. [Electronic version]. *Washington Technology*. Retrieved 5/19/2009
- Lipowicz, A. (2007a, September 25). ITAA to congress: Cut a check for Real ID now. *Washington Technology*. Retrieved 11/9/2007, from [http://www.washingtontechnology.com/online/1\\_1/31487-1.html](http://www.washingtontechnology.com/online/1_1/31487-1.html)
- Lipowicz, A. (2007b, August 3). Mixed signs: A lack of federal funding for Real ID leaves states in the lurch. *Washington Technology*. Retrieved 8/1/2009 from <http://washingtontechnology.com/Articles/2007/08/03/Mixed-signs.aspx>
- Lipowicz, A. (2007c, July 25). At DHS, risk assessment backlog looms. *Washington Technology*. Retrieved 9/15/2007 from [http://www.washingtontechnology.com/online/1\\_1/31108-1.html](http://www.washingtontechnology.com/online/1_1/31108-1.html)
- Lipowicz, A. (2007d, February 12). DHS tunes out RFID. *Washington Technology*. Retrieved 5/19/2009 from <http://washingtontechnology.com/articles/2007/02/12/dhs-tunes-out-rfid.aspx>
- Lippmann, W. (1922). *Public opinion*. New York: Macmillan.
- Liu, L.H. (1995). *Translingual practice: Literature, national culture, and translated modernity--China, 1900-1937*. Stanford, Calif.: Stanford University Press.
- Longman, T. (2001). Identity cards, ethnic self-perception, and genocide in Rwanda. In J. Caplan, & J. Torpey (Eds.), *Documenting individual identity: The development of state practices in the modern world* (pp. 345-358). Princeton, N.J.: Princeton University Press.
- Los, M. (2006). Looking into the future: Surveillance, globalization and the totalitarian potential. In D. Lyon (Ed.), *Theorizing surveillance* (). Ontario: Willan Publishing.
- Lu, X., & Perry, E.J. (1997). *Danwei: The changing Chinese workplace in historical and comparative perspective*. Armonk, N.Y.: M. E. Sharpe.

- Lu, Y. (2005). Privacy and data privacy issues in contemporary China. *Ethics and Information Technology*, 7, 7-15.
- Lyon, D. (2007a). *Surveillance studies: An overview*. Cambridge, UK; Malden, MA: Polity.
- Lyon, D. (2007b). National ID cards: Crime-control, citizenship and social sorting. *Policing*, 1(1), 111.
- Lyon, D. (2004). Globalizing surveillance: Comparative and sociological perspectives. *International Sociology*, 19(2), 135-149.
- Lyon, D. (2002). Surveillance studies: Understanding visibility, mobility and the phenetic fix. *Surveillance and Society*, 1(1).
- Lyon, D. (2001). New directions in theory. *Surveillance society: Monitoring everyday life* Buckingham [England]; Philadelphia: Open University. 189 p.
- Madsen, R. (2007). Confucian conceptions of civil society. In D. Bell (Ed.), *Confucian political ethics* (p. 3). Princeton: Princeton University Press.
- Margulis, S. T. (2003). On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues*, 59(2), 411-429.
- Markoff, J. (2002, November 9). Pentagon plans a computer system that would peek at personal data of Americans. *The New York Times*. Retrieved 7/23/09 from <http://www.nytimes.com/2002/11/09/politics/09COMP.html>
- Marshals: Innocent people placed on 'watch list' to meet quota. (2006, July 21). Retrieved 2/26/2009 from <http://www.thedenverchannel.com/news/9559707/detail.html>
- Martinsen, J. (2007). *Mr. Sun, I'll need to see some ID*. Retrieved 5/9/2009, from [http://www.danwei.org/ip\\_and\\_law/mr\\_sun\\_ill\\_need\\_to\\_see\\_some\\_id.php](http://www.danwei.org/ip_and_law/mr_sun_ill_need_to_see_some_id.php)
- Marx, G.T. (2005). Surveillance and Society. Encyclopedia of Social Theory. Retrieved 8/12/09 from <http://web.mit.edu/gtmarx/www/surandsoc.html>
- Marx, G. T. (2002). What's new about the "New surveillance"? classifying for change and continuity. *Surveillance & Society*, 1(1), 9-29.

- Marx, G. T. (2001). Murky conceptual waters: The public and the private. *Ethics and Information Technology*, 3(3), 157-169.
- Matthews, W. (2002, July 29). Ashcroft: No central database for citizen tips. [Electronic version]. *Federal Computer Week*. Retrieved 5/2/2008 from <http://fcw.com/articles/2002/07/29/ashcroft-no-central-database-for-citizen-tips.aspx>
- McCullagh, D. (2008, September 12). U.N. agency eyes curbs on internet anonymity. Retrieved 5/10/ 2009 from [http://news.cnet.com/8301-13578\\_3-10040152-38.html](http://news.cnet.com/8301-13578_3-10040152-38.html)
- McDougall, B.S. (2002). Particulars and universals: Studies on Chinese privacy. In B. S. McDougall, & A. Hansson (Eds.), *Chinese concepts of privacy* (p. 3). Netherlands; Boston: Brill.
- McDougall, B.S., & Hansson, A. (2002). *Chinese concepts of privacy*. Leiden Netherlands; Boston: Brill.
- McLuhan, M. (1964). Introduction, in *The bias of communication*. Innis, H. A. Toronto: University of Toronto Press.
- McNamara, T. E. (2006, November). *Information sharing environment implementation plan*. U.S. Information Sharing Environment (ISE).
- Meyerson, H. (2007, September 19, 2007). China's hot stock: Orwell, inc. *Washington Post*, p. A23.
- Meyrowitz, J. (1985). *No sense of place: The impact of electronic media on social behavior*. New York: Oxford University Press.
- Meet the national joint terrorism task force. (2004). Retrieved 3/21, 2009 from <http://www.fbi.gov/page2/july04/njtff070204.htm>
- Miller, J. (2007, December 7). DOJ tests suspicious-activity reporting system. [Electronic version]. *Federal Computer Week*. Retrieved 11/13/08 from [http://www.fcw.com/online/news/151032-1.html?topic=state\\_and\\_local](http://www.fcw.com/online/news/151032-1.html?topic=state_and_local)

- Minister of public security explains need for identity cards. (1985, June 13). *Xinhua news, from BBC Summary of World Broadcasts*.
- Monahan, T. (2006). Counter-surveillance as political intervention? *Social Semiotics*, 16(4), 515-534; 515.
- Moore, B. (2007). AIM viewpoint: "real ID" reality check. Retrieved 4/13, 2009 from <http://www.aimglobal.org/members/news/templates/template.aspx?articleid=2312&zoneid=26>
- Moore, B. (1997). *Victims and survivors: The Nazi persecution of the Jews in the Netherlands, 1940-1945*. London; New York: Arnold.
- Moring, R. (2009, March 26). Missouri highway patrol rescinds controversial militia report. [Electronic version]. *St. Louis Post Dispatch*. Retrieved 4/27/2009 from <http://www.stltoday.com/stltoday/news/stories.nsf/missouristatenews/story/A8718605909247EB862575850003B8B4?OpenDocument>
- Morville, P. (2005). *Ambient findability* (1st ed.). Beijing; Sebastopol, CA: O'Reilly.
- Myers, L., Pasternak, D., & Gardella, R. (2005, Dec. 14). Is the Pentagon spying on Americans? [Electronic version]. *MSNBC.com*. Retrieved 6/18/2009 from <http://www.msnbc.msn.com/id/10454316/>
- Myers, R.B. (2004, May 12). The President's FY05 Budget Request for the Department of Defense: Hearings before the Defense Subcommittee, Senate Committee on Appropriations, U.S. Senate. Testimony. Chairman, Joint Chiefs of Staff.
- Myers, R.B. (2004, May 11). Chairman, Joint Chiefs of Staff Remarks to the AFCEA TechNet International 2004 Conference "Combating Emerging Threats", Washington, DC Convention Center. Retrieved 7/20/2009 from [http://www.cellexchange.com/News/Articles/JPEN/JPEN\\_004.pdf](http://www.cellexchange.com/News/Articles/JPEN/JPEN_004.pdf)
- Mueller, R.S. (2005). Federal bureau of investigation's information technology modernization program, trilogy. Hearings before the Committee on Senate Appropriations, U.S. Senate,

- S. Hrg 109-76 Sess. (2005). (Testimony of Robert S. III Mueller. ) Retrieved 6/12/09 from [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109\\_senate\\_hearings&docid=f:20668.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_senate_hearings&docid=f:20668.pdf)
- Nakashima, E. (2008, January 1). Electronic passports raise privacy issues. [Electronic version]. *Washington Post*, pp. n.p. Retrieved 5/19/2009 from <http://www.washingtonpost.com/wp-dyn/content/article/2007/12/31/AR2007123101922.html>
- Nakashima, E. (2007, July 11). FBI plans initiative to profile terrorists. [Electronic version]. *Washington Post*, Retrieved 6/14/2009 from <http://www.washingtonpost.com/wp-dyn/content/article/2007/07/10/AR2007071001871.html>
- Nakashima, E., & Hsu, S. S. (2006, November 3). U.S. plans to screen all who enter, leave country. [Electronic version]. *Washington Post*, pp. A18. Retrieved 11/12/08 from <http://www.washingtonpost.com/wp-dyn/content/article/2006/11/02/AR2006110201810.html>
- National ID project moves China to head of the pack in radio frequency technology. (2007, February 21). [Electronic version]. *Card Technology*. Retrieved 1/24/2009 from <http://www.cardtechnology.com/article.html?id=20070221PGYABPF5>
- “National network” of fusion centers raises specter of COINTELPRO. (2007). Retrieved 6/23, 2009, from <http://epic.org/privacy/surveillance/spotlight/0607/default.html>
- New ID card ensures privacy. (2006, February 10). [Electronic version]. *Shenzhen Daily*. Retrieved 5/12/09 from [http://english.gov.cn/2006-02/10/content\\_184763.htm](http://english.gov.cn/2006-02/10/content_184763.htm)
- Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79(1), 119-157.
- Nissenbaum, H. (1998). Protecting privacy in an information age: The problem of privacy in public. *Law and Philosophy*, 17, 559-596.
- Norris, C. (2003). From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control. In D. Lyon (Ed.), *Surveillance as social*



- sorting: Privacy, risk, and digital discrimination* (pp. 249-281). London; New York: Routledge.
- O'Harrow, R. (2008, April 2). Centers tap into personal databases. *Washington Post*, pp. A01.
- O'Harrow, R. (2006). *No place to hide* (1st Free Press trade pbk. ed.). New York: Free Press.
- O'Kane, B. (2005). *University BBS explodes with snark*. Retrieved 5/10/2009 from [http://www.danwei.org/internet/university\\_bbs\\_explodes\\_with\\_s.php](http://www.danwei.org/internet/university_bbs_explodes_with_s.php)
- Olmsted, K. S. (1996). *Challenging the secret government: The post-watergate investigations of the CIA and FBI*. Chapel Hill: University of North Carolina Press.
- Orzech, D. (2003). *Rapidly falling storage costs mean bigger databases, new applications*. Retrieved 3/1, 2008 from <http://www.enterprisestorageforum.com/technology/features/article.php/2248651>
- Palen, L., & Dourish, P. (2003). Unpacking "privacy" for a networked world. *ACM Conference on Human Factors in Computing Systems*, Fort Lauderdale, FL.
- Passerin d'Entrèves, M., & Vogel, U. (2000). *Public and private: Legal, political and philosophical perspectives*. London; New York: Routledge.
- Patient's privacy rights become an issue in China.(2001, July 17). [Electronic version]. *China Daily*. Retrieved March 1, 2008 from <http://french.10thnpc.org.cn/english/features/aids/113315.htm>
- Pentagon's 'Terror Information Awareness' program will end. (2003, September 25). Retrieved 7/20/09 from [http://www.usatoday.com/news/washington/2003-09-25-pentagon-office\\_x.htm](http://www.usatoday.com/news/washington/2003-09-25-pentagon-office_x.htm)
- Peerenboom, R.P. (2002). *China's long march toward rule of law*. Cambridge, UK; New York: Cambridge University Press.
- Pels, D. (2002). Everyday essentialism. Social inertia and the Münchhausen effect. *Theory, Culture & Society*, 19(5/6), 69-89.

- Pentagon statement on domestic intelligence surveillance. (2005). Retrieved 6/18/2009 from <http://fas.org/sgp/news/2005/12/dod121405.html>
- Petronio, S. S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany: State University of New York Press.
- Perrin, C. (2009). *Why REAL ID is not secure ID*. Retrieved 7/23/2009 from <http://blogs.techrepublic.com.com/security/?p=1590>
- Phillips, D. J. (2004). Privacy policy and PETs - the influence of policy regimes on the development and social implications of privacy enhancing technologies. *New Media & Society*, 6(6), 691-706.
- Photo, ID now required to use Beijing internet cafes.(2008, October 16). *Xinhua*.
- Piatetsky-Shapiro, G. (1999). The data-mining industry coming of age. *IEEE Intelligent Systems*, (November/December) 32-34.
- Pincus, W. (2007, April 25). Pentagon to end talon data-gathering program. [Electronic version]. *Washington Post*. Retrieved 2/15/08 from <http://www.washingtonpost.com/wp-dyn/content/article/2007/04/24/AR2007042402540.html?hpid=sec-nations>
- Pincus, W. (2005, November 27). Pentagon expanding its domestic surveillance activity. *Washington Post*.
- Plowright, A. (2008). *Is mobile network big brother surveillance tool?* Retrieved 5/10/2009 2009, from <http://www.chinapost.com.tw/china/2008/01/28/140851/Is-mobile.htm>
- Poll exposes generational divide on privacy expectations.(2007, February 1). [Electronic version]. *Government Technology*. Retrieved 9/12/08 from <http://www.govtech.com/gt/articles/103678>
- Porter, J., & Crumley, J. (2006, April). Joint protection enterprise network. *Military Police*, 26-27.
- Posner, R.A. (2006). *Not a suicide pact: The constitution in a time of national emergency*. New York; Oxford: Oxford University Press.

- Posner, R.A. (1978). The right of privacy. *Georgia Law Review*, 12(3), 393-422.
- Poster, M. (1996). Databases as discourse; or, electronic interpellations. In D. Lyon, & E. Zureik (Eds.), *Computers, surveillance, and privacy* (pp. 175-192; 9). Minneapolis: University of Minnesota Press.
- Poster, M. (1990). *The mode of information: Poststructuralism and social context*. Chicago: University of Chicago Press.
- Privacy office - DHS data privacy and integrity advisory committee. (2009). Retrieved 7/20/2009 from [http://www.dhs.gov/files/committees/editorial\\_0512.shtm](http://www.dhs.gov/files/committees/editorial_0512.shtm)
- Privacy act overview, May 2004 edition: Social security number usage. (2004). Retrieved 5/24/2009, from <http://www.usdoj.gov/opcl/1974ssnu.htm>
- Privacy's gap: The largely non-existent legal framework for government mining of commercial data. (2003, May 28). Center for Democracy & Technology. Retrieved February 10, 2007 from <http://www.cdt.org/security/usapatriot/030528cdt.pdf>.
- Protecting individual privacy in the struggle against terrorists: A framework for program assessment. (2008). Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, National Research Council. Retrieved 1/10/2009 from [http://www.nap.edu/catalog.php?record\\_id=12452](http://www.nap.edu/catalog.php?record_id=12452)
- Qiang, G. (2006). 'Temporary residence permit system illegal'. Retrieved 11/13/2007, 2007, from [http://www.chinadaily.com.cn/china/2006-12/27/content\\_769202.htm](http://www.chinadaily.com.cn/china/2006-12/27/content_769202.htm)
- Qiu, J. L., & Hachigian, N. (2004). *A new long march: E-government in China*. OECD.
- Qu, L. (2008, January 10). Baidu and HiChina found not guilty. Retrieved March 15, 2008 from [http://www.pacificepoch.com/newsstories/114120\\_0\\_5\\_0\\_M/](http://www.pacificepoch.com/newsstories/114120_0_5_0_M/)
- Quinn, T. D. (2006, February). Tactical information sharing system. [Electronic version]. *The Police Chief*. Retrieved 7/10/09 from [http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display\\_arch&article\\_id=810&issue\\_id=22006](http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=810&issue_id=22006)

- Ramasastri, A. (2005). *Why the 'Real ID' Act is a real mess*. Retrieved 5/15/2009, from <http://www.cnn.com/2005/LAW/08/12/ramasastri.ids/index.html>
- Rankin, M. B. (1993). Some observations on a Chinese public sphere. *Modern China*, 19(2), Symposium: "Public Sphere"/"Civil Society" in China? Paradigmatic Issues in Chinese Studies, III, 158-182.
- The Real ID Act: National impact analysis*. National Governors Association; National Conference of State Legislators; American Association of Motor Vehicle Administrators. (2006). September. Retrieved 5/1/09 from <http://www.nga.org/Files/pdf/0609REALID.PDF>.
- Real ID: Threatening your privacy through an unfunded government mandate. (n.d.). Retrieved 5/19/2009 from <http://www.eff.org/issues/real-id>
- RealID snippet unverified*. Retrieved 5/12/09 from [http://www.wired.com/images\\_blogs/threatlevel/files/realidsnippetunverified.txt](http://www.wired.com/images_blogs/threatlevel/files/realidsnippetunverified.txt)
- Real-name online registration system meets opposition in china.(2007, January 9). [Electronic version]. *People's Daily*, Retrieved October 2, 2007 from [http://english.peopledaily.com.cn/200701/09/eng20070109\\_339327.html](http://english.peopledaily.com.cn/200701/09/eng20070109_339327.html)
- Reimer, J. (2007, March 15). Your ISP may be selling your web clicks. [Electronic version]. *Ars Technica*. Retrieved 7/2/2009 from <http://arstechnica.com/tech-policy/news/2007/03/your-isp-may-be-selling-your-web-clicks.ars>
- Reder, M. (1999). Some other paradigms. *Economics: The culture of a controversial science* (pp. 108-141) University of Chicago Press.
- RFID in China - the biggest RFID market this year. (2007, August 23). [Electronic version]. *IDTechEx*. Retrieved 2/6/2009 from [http://www.idtechex.com/research/articles/rfid\\_in\\_china\\_the\\_biggest\\_rfid\\_market\\_this\\_year\\_00000673.asp](http://www.idtechex.com/research/articles/rfid_in_china_the_biggest_rfid_market_this_year_00000673.asp)
- RFID in China. (2006, August 30). [Electronic version]. *IDTechEx*. Retrieved 3/14/2009 from [http://www.idtechex.com/research/articles/rfid\\_in\\_china\\_00000491.asp](http://www.idtechex.com/research/articles/rfid_in_china_00000491.asp)

- Robins, K., & Webster, F. (1999). The long history of the information revolution. *Times of the technoculture : From the information society to the virtual life* (pp. 89-110). London; New York: Routledge & K. Paul.
- Rorty, R. (1989). *Contingency, irony, and solidarity*. Cambridge; New York: Cambridge University Press.
- Rothschild, M. (2008a, July 2). The new snoops: Terrorism liaison officers, some from private sector. [Electronic version]. *The Progressive*. Retrieved 9/22/08 from <http://www.progressive.org/mag/mc070208>
- Rothschild, M. (2008b, March). The FBI deputizes business. [Electronic version]. *The Progressive*. Retrieved January 10, 2009 from [http://www.progressive.org/mag\\_rothschild0308](http://www.progressive.org/mag_rothschild0308)
- Rosemont, H., JR. (1974). On representing abstractions in archaic Chinese. *Philosophy East and West*, 24(1), 71-88.
- Rowe, W.T. (1990). The public sphere in modern China. *Modern China*, 16(3), 309-329.
- Rule, J. B. (2007). *Privacy in peril*. Oxford; New York: Oxford University Press.
- Rule, J. B., McAdam, D., Stearns, L., & Uglow, D. (1983). Documentary identification and mass surveillance in the United States. *Social Problems*, 31(2), 222-234.
- Safire, W. (2002, November 14). You Are a Suspect. *The New York Times*. Retrieved 7/20/08 from <http://www.nytimes.com/2002/11/14/opinion/14SAFI.html>.
- Saiz, A., & Simonsohn, U. (2007). *Downloading wisdom from online crowds. working paper*. Unpublished manuscript. Retrieved 3/21/2009 from <http://ssrn.com/abstract=990021>
- Salmond, A. (1982). Theoretical landscapes: A cross-cultural conception of Knowledge . In D. J. Parkin (Ed.), *Semantic anthropology* (pp. 65-88). London; New York: Academic Press.

Schneier, B. (2008). *The NSA teams up with the Chinese government to limit internet anonymity*.

Retrieved 5/10/2009 from

[http://www.schneier.com/blog/archives/2008/09/the\\_nsa\\_teams\\_u.html](http://www.schneier.com/blog/archives/2008/09/the_nsa_teams_u.html)

Schneier, B. (2007a, September 20). Lesson from Tor hack: Anonymity and privacy aren't the

same. [Electronic version]. *Wired*, Retrieved March 1, 2008 from

[http://www.wired.com/print/politics/security/commentary/securitymatters/2007/09/security\\_matters\\_0920](http://www.wired.com/print/politics/security/commentary/securitymatters/2007/09/security_matters_0920)

Schneier, B. (2007b) Will real ID actually make us safe? an examination of civil liberties

concerns: Hearings before the Senate Judiciary Committee, Will real ID actually make us

safe? an examination of civil liberties concerns: (2007). (Testimony) Retrieved 7/1/09

from <http://www.schneier.com/testimony-realid.html>

Schon, D. Generative metaphor: (1979). A perspective on problem setting in social policy. In A.

Ortony (Ed.), *Metaphor and thought* (pp. 137-163). Cambridge; New York: Cambridge

University Press.

Searle, J.R. (1995). *The construction of social reality*. New York: Free Press.

Seifert, J. W., & Chung, J. (2009). Using E-government to reinforce government, citizen

relationships: Comparing government reform in the United States and China. *Social*

*Science Computer Review*, 27(3). Retrieved December 1, 2008 from

<http://ssc.sagepub.com/cgi/content/abstract/27/1/3>

Sewell, D. (2006, October 4). Court allows government to keep surveillance for now. *AP*.

Shaw, V. N. (1996). *Social control in China: A study of Chinese work units*. Westport, Conn.:

Praeger.

Shanghai subway authorities apologize over leaked kiss video. (2008, January 25). [Electronic

version]. *Xinhua*. Retrieved March 15, 2008 from

[http://news.xinhuanet.com/english/2008-01/25/content\\_7495781.htm](http://news.xinhuanet.com/english/2008-01/25/content_7495781.htm)

- Shapiro, S. (1998). Places and spaces: The historical interaction of technology, home, and privacy. *Information Society*, 14(4), 275-284.
- Shi, Y. (2002). *The establishment of modern Chinese grammar: The formation of the resultative construction and its effects*. Amsterdam; Philadelphia: John Benjamins Pub. Co.
- Shorrock, T. (2008). *Spies for hire: The secret world of intelligence outsourcing* (1 Simon & Schuer hacover ed.). New York: Simon & Schuster.
- Shuy, R. (2008). *Person of interest*. Retrieved 6/12, 2009 from <http://languagelog.ldc.upenn.edu/nll/?p=317>
- Singel, R. (2007a, November 12). Spy official calling anonymity dead simply summarizing gov spying powers. [Electronic version]. *Wired*. Retrieved January 10, 2008 from <http://blog.wired.com/27bstroke6/2007/11/spy-official-ca.html>
- Singel, R. (2007b, September 20). U.S. airport screeners are watching what you read. [Electronic version]. *Wired*. Retrieved October 12, 2007 from [http://www.wired.com/politics/onlinerights/news/2007/09/flight\\_tracking](http://www.wired.com/politics/onlinerights/news/2007/09/flight_tracking)
- Singel, R. (2007c, July 6). Appeals court rules no privacy interest in IP addresses, email To/From fields. [Electronic version]. *Wired*. Retrieved March 1, 2008 from <http://blog.wired.com/27bstroke6/2007/07/appeals-court-r.html>
- Singel, R. (2007d, January 17). *National ID to be privatized, activist says he has docs*. Retrieved 5/15/2009 from [http://www.wired.com/threatlevel/2007/01/national\\_id\\_to\\_/](http://www.wired.com/threatlevel/2007/01/national_id_to_/)
- Singel, R. (2006, October 30). Feds leapfrog RFID privacy study. *Wired*. Retrieved 6/13/2009 from <http://www.wired.com/science/discoveries/news/2006/10/72019>
- Sklar, H. (1988). *Washington's war on Nicaragua*. Boston, MA: South End Press.
- Smith, R. E. (2006, December 6). Beware demands for your social security number. [Electronic version]. *Forbes*, Retrieved 5/18/2009 from [http://www.forbes.com/2006/12/05/social-security-identity-theft-oped-cx\\_res\\_1206smith.html](http://www.forbes.com/2006/12/05/social-security-identity-theft-oped-cx_res_1206smith.html)

- Smith, R. E. (2004). The social security number in America: 1935-2000. In C. Watner, & W. McElroy (Eds.), *National identification systems: Essays in opposition* (pp. 203-222). Jefferson, N.C.; London: McFarland & Co.
- Snow, David A.m Benford, and Robert D. (1992). Master frames and cycles of protest. In A. D. Morris, & C. M. Mueller (Eds.), *Frontiers in social movement theory* (pp. 133-155). New Haven, Conn.: Yale University Press.
- Sobel, R. (2002). The degradation of political identity under a national identification system. *Boston University Journal of Science and Technology Law*, 8(1), 37-56.
- Solove, D. J. (2007). *The future of reputation: Gossip, rumor, and privacy on the internet*. New Haven: Yale University Press.
- Solove, D. J. (2006). A brief history of information privacy law. In C. Wolf (Ed.), *Proskauer on privacy* (pp. 1). New York: Practising Law Institute.
- Solove, D.J. (2004). *The digital person: Technology and privacy in the information age*. New York: New York University Press.
- Solove, D. J. (2002). Digital dossiers and the dissipation of fourth amendment privacy. *Southern California Law Review*, 75, 1083.
- Sowa, J. (2002). Semantic networks. Retrieved 3/21, 2009 from <http://jfsowa.com/pubs/semnet.htm>
- Stake, R. E. (2000). Case studies. In N. K. Denzin, & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (2nd ed., pp. 435). Thousand Oaks, Calif.: Sage Publications.
- Stake, R. E. (1995). *The art of case study research*. Thousand Oaks, Calif.: Sage Publications.
- Stalder, F., & Lyon, D. (2003). Electronic identity cards and social classification. In D. Lyon (Ed.), *Surveillance as social sorting: Privacy, risk, and digital discrimination* (pp. 77). London; New York: Routledge.
- Stanley, J. (2004, August). The surveillance-industrial complex: How the American government is conscripting businesses and individuals in the construction of a surveillance society.



- American Civil Liberties Union (ACLU). Retrieved 1/22/2009 from [http://www.aclu.org/FilesPDFs/surveillance\\_report.pdf](http://www.aclu.org/FilesPDFs/surveillance_report.pdf) ).
- State groups acknowledge final real ID regulations. (2008). Retrieved 6/13/2009 from <http://www.nga.org/portal/site/nga/menuitem.6c9a8a9ebc6ae07eee28aca9501010a0/?vgnextoid=618752ad9b567110VgnVCM1000001a01010aRCRD>
- Stein, J. (2006). Sure, the FBI's computers have problems, but look what they have on me. Retrieved 11/13/2007 from [http://public.cq.com/public/20060224\\_homeland.html](http://public.cq.com/public/20060224_homeland.html)
- Stokes, J. (2008). Analysis: Metcalfe's law + real ID = more crime, less safety. Retrieved 5/29/2009 from <http://arstechnica.com/tech-policy/news/2008/01/analysis-metcalfes-law-real-id-more-crime-less-safety.ars>
- Strand, D. (1989). *RickshawBeijing: City people and politics in the 1920s*. Berkeley: University of California Press.
- Su, N. (2007, October 16). Remarks at the Press Conference on the inauguration of the Online Verification of Citizens' Identity Information. Retrieved 7/12/09 from <http://www.pbc.gov.cn/english/detail.asp?col=6500&ID=153>
- Sullivan, E. (2008, April 11). LAPD looks to uncover terrorist plots. [Electronic version]. *AP*. Retrieved 12/2/2008 from [http://www.usatoday.com/news/washington/2008-04-11-3032705408\\_x.htm](http://www.usatoday.com/news/washington/2008-04-11-3032705408_x.htm)
- Sundstrom, S. A. (1998). You've got mail-- (and the government knows it): Applying the fourth amendment to workplace E-mail monitoring. *New York University Law Review*, 73, 2064.
- Swearingen, M. W. (1995). *FBI secrets: An agent's exposé*. Boston, MA: South End Press.
- Tai, J.H.Y., & Chan, M.K.M. (1999). Some reflections on the periodization of the Chinese language. In A. Peyraube, & C. Sun (Eds.), *Studies in Chinese historical syntax and morphology: Linguistic essays in honor of Mei Tsu-lin* (pp. 223-239). Paris: Ecole des Hautes Etudes en Sciences Sociales.

- Taking steps to further improve our privacy practices. (2007, March 13). *The Official Google Blog*. Retrieved May 12, 2008, from <http://googleblog.blogspot.com/2007/03/taking-steps-to-further-improve-our.html>
- Tang, W. (2005). *Public opinion and political change in China*. Stanford, Calif.: Stanford University Press.
- Tarrow, S. G. (1994). *Power in movement: Social movements, collective action, and politics*. Cambridge England; New York: Cambridge University Press.
- The president v. congress: Signing statements and non-enforcement. (2006). American Bar Association.
- Tiller, E. H., & Cross, F. (2005). *What is legal doctrine? what is legal doctrine?* Northwestern Public Law Research Paper No. 05-06.
- Time to stop tinkering with “watch lists.” (2009). Retrieved 6/12/2009 from <http://www.papersplease.org/wp/2009/05/18/time-to-stop-tinkering-with-watchlists/>
- Todd, R. S. (2006). *FBI's new data warehouse a powerhouse*. Retrieved 4/12, 2009 from <http://www.cbsnews.com/stories/2006/08/30/terror/main1949643.shtml>
- Treverton, G. F. (2008). *Reorganizing U.S. domestic intelligence: Assessing the options*. RAND Corporation. Prepared for the Department of Homeland Security. 151 pages.
- Tucker, R. C. (1965). The dictator and totalitarianism. *World Politics*, 17(4), 555-583.
- Turow, J. (2006). *Niche envy: Marketing discrimination in the digital age*. Cambridge, Mass.: MIT Press.
- Twight, C. (2004). Systematic federal surveillance of ordinary Americans. In C. Watner, & W. McElroy (Eds.), *National identification systems: Essays in opposition* (pp. 147-183). Jefferson, N.C.: McFarland & Co.
- U.S. Congressional Research Service (CRS) (2007, March 20). National Security Letters in Foreign Intelligence Investigations: A Glimpse of the Legal Background and Recent

- Amendments. Retrieved 7/20/2009 from <http://opencrs.com/document/RS22406/2007-03-20%2000:00:00>
- U.S. Department of Defense (DOD), Office of the Inspector General. (2007, June 27). *The threat and local observation notice (TALON) program* No. 07-INTEL-09.
- U.S. Department of Defense (DOD), Deputy Secretary of Defense Gordon England (2006, March 30). Threats to the Department of Defense (DOD). Memorandum. Retrieved 7/25/09 from <http://www.fas.org/irp/agency/dod/033006talon.pdf>
- U.S. Department of Defense (DOD), Deputy Secretary of Defense Paul Wolfowitz (2003, May 2). Collection, reporting and analysis of terrorist threats within the United States. Memorandum. Retrieved 7/24/09 from <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB230/04.pdf>
- U.S. Department of Homeland Security (DHS). (2007). *REAL ID proposed guidelines: Questions & answers*. Retrieved 12/5/07 from [http://www.dhs.gov/xprevprot/laws/gc\\_1172767635686.shtm](http://www.dhs.gov/xprevprot/laws/gc_1172767635686.shtm)
- U.S. Department of Homeland Security (DHS), Data Privacy & Integrity Advisory Committee, Emerging Applications and Technology Subcommittee. (2006, October). The Use of RFID for Human Identification. A DRAFT REPORT, Version 1.0. Retrieved 5/12/09 from [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_advcom\\_rpt\\_rfid\\_draft.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_rpt_rfid_draft.pdf)
- U.S. Department of Homeland Security (DHS). (2005). Homeland sec. advisory council, summary of meeting: December 14, 2004. March 7.
- U.S. Department of Justice (DOJ) (n.d.). *Fusion center guidelines: Developing and sharing information and intelligence in a new era*. Guidelines. Retrieved 2/22/09 from [http://www.it.ojp.gov/documents/fusion\\_center\\_guidelines\\_law\\_enforcement.pdf](http://www.it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf).
- U.S. Department of Justice (DOJ), Office of the Inspector General (2008, November). The Federal Bureau of Investigation's terrorist threat and suspicious incident tracking system. No. 09-02. Retrieved 02/02/09 from <http://www.usdoj.gov/oig/reports/FBI/a0902/final.pdf>.

- U.S. Department of Justice (DOJ) Office of the Inspector General (2008, March). A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006. Retrieved 7/20/09 from <http://www.usdoj.gov/oig/special/s0803b/final.pdf>
- U.S. Department of Justice (DOJ), Office of the Inspector General, Audit Division (2007, September). Follow-up audit of the Terrorist Screening Senter. Audit Report 07-41.
- U.S. Department of Justice (DOJ), Office of the Inspector General (2005, September). The Federal Bureau of Investigation's Compliance with the Attorney General's Investigative Guidelines (Redacted). Chapter Two: Historical Background of the Attorney General's Investigative Guidelines. Retrieved 7/20/09 from <http://www.usdoj.gov/oig/special/0509/chapter2.htm>
- U.S. Department of Treasury (DOT), Office of the Comptroller of the Currency. (2000). *Bank secrecy Act/Anti-money laundering (Comptroller's handbook)* (Consumer Compliance Examination No. CCE-BSA). December. Retrieved 7/12/09 from <http://www.occ.treas.gov/handbook/bsa.pdf>.
- U.S. Federal Bureau of Investigation (FBI) (2004, April 14). Report to the national commission on terrorist attacks upon the United States: The FBI's counterterrorism program since September 2001. Retrieved 3/5/09 from <http://www.fbi.gov/publications/commission/9-11commissionrep.pdf>.
- U.S. Federal Trade Commission (FTC). (2006). *President's identity theft task force: Summary of interim recommendations*. September 16. Retrieved 5/1/09 from <http://www.ftc.gov/os/2006/09/060916interimrecommend.pdf>.
- U.S. Government Accountability Office (GAO). 2008, September 9. Aviation security: TSA is enhancing its oversight of air carrier efforts to screen passengers against terrorist watch-list records, but expects ultimate solution to be implementation of Secure Flight. Statement of Cathleen A. Berrick, Director, Homeland Security and Justice Issues.

Testimony before the Subcommittee on Transportation Security and Infrastructure Protection, Committee on Homeland Security, House of Representatives. GAO-08-1136T.

U.S. Government Accountability Office (GAO). (2007, January 31). BORDER SECURITY:

U.S.-VISIT program faces strategic, operational, and technological challenges at land ports of entry. No. GAO-07-378T.

U.S. Government Accountability Office (GAO). (2007, October). Terrorist watch list screening:

Opportunities exist to enhance management oversight, reduce vulnerabilities in agency screening processes, and expand use of the list (Report to Congressional Requesters No. GAO-08-110). Retrieved November 1, 2007 from

<http://www.gao.gov/new.items/d08110.pdf>.

U.S. Government Accountability Office (GAO). (2007). HOMELAND SECURITY: Federal

efforts are helping to alleviate some challenges encountered by state and local information fusion centers No. GAO-08-35. October. Retrieved 7/12/09 from

<http://www.gao.gov/new.items/d0835.pdf>.

U.S. Government Accountability Office (GAO) (2006, June 12). International Financial Crime:

Treasury's Roles and Responsibilities Relating to Selected Provisions of the USA PATRIOT Act No. GAO-06-483. October. Retrieved 7/12/09 from

<http://www.gao.gov/new.items/d0835.pdf>.

U.S. Department of Health, Education, and Welfare (HEW) (1973, July). Records, Computers

and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems. Retrieved 7/20/09 from

<http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm>

U.S. Information Awareness Office (IAO) U.S. Department of Defense (DOD), Defense

Advanced Research Projects Agency (2002, July 19). Total Information Awareness

- Program (TIA) System Description Document (SDD) Version 1.1. Retrieved 7/20/09 from <http://epic.org/privacy/profiling/tia/tiasystemdescription.pdf>
- U.S. Office of the Director of National Intelligence (DNI). 2008. Information sharing environment (ISE) functional standard (FS), suspicious activity reporting (SAR) version 1.0. (ISE-FS-200). January, 28.
- U.S. Social Security Administration (SSA). Social security number chronology of history. Retrieved 5/7/09 from <http://www.ssa.gov/history/ssn/ssnchron.html>.
- Ure, J., & Liang, X. J. (2000). Convergence and China's national information infrastructure. In M. A. Hukill, R. Ono & C. Vallath (Eds.), *Electronic communication convergence: Policy challenges in Asia* (pp. 115-147). New Delhi; Thousand Oaks, Calif.: Sage Publications.
- Venuti, L. (1998). *The scandals of translation: Towards an ethics of difference*. London; New York: Routledge.
- Villeneuve, N. (2008). *TOM-skype Q & A*. Retrieved 5/10/2009, 2009, from <http://www.nartv.org/2008/10/02/tom-skype-q-a/>
- Vijayan, J. (2007, May 11). DHS privacy committee joins real ID opposition. [Electronic version]. *InfoWorld*, 2009. Retrieved 7/23/2009 from <http://www.infoworld.com/d/security-central/dhs-privacy-committee-joins-real-id-opposition-080>
- Wakeman Jr., F. (1998). Boundaries of the public sphere in Ming and Qing China. *Daedalus*, 127(3), 167.
- Wang, Z. (2005). Political trust in China: Forms and causes. In L. White (Ed.), *Legitimacy: Ambiguities of political success of failure in East and Southeast Asia* (pp. 113-139). Singapore: World Scientific.
- Walder, A. G. (1987). Communist social structure and worker's politics in China. In V. C. Falkenheim (Ed.), *Citizens and groups in contemporary China* (pp. 45-90). Ann Arbor: Center for Chinese Studies, University of Michigan.

- Walton, G. (2001). *China's golden shield: Corporations and the development of surveillance technology in the people's republic of China*. Montréal: International Centre for Human Rights and Democratic Development.
- Washington post-ABC news poll*. (2006). Retrieved 1/18, 2008 from [http://www.washingtonpost.com/wp-srv/politics/polls/postpoll\\_nsa\\_051](http://www.washingtonpost.com/wp-srv/politics/polls/postpoll_nsa_051)
- Wang, F. (2005). *Organizing through division and exclusion: China's hukou system*. Stanford, Calif.: Stanford University Press.
- Wang, F. (2004). Reformed migration control and new targeted people: China's hukou system in the 2000s. *The China Quarterly*, (177), 115-132.
- Wark, M. (1994). *Virtual geography: Living with global media events*. Bloomington: Indiana University Press.
- Watner, C. (2004). Driver's licenses and vehicle registration in historical perspective. In C. Watner, & W. McElroy (Eds.), *National identification systems: Essays in opposition* (pp. 101-115) .
- Weigel, D. (2008, October). Who killed Real ID?: An unlikely coalition wins a post-9/11 victory for civil liberties. [Electronic version]. *Reason Magazine*. Retrieved 5/15/2009 from <http://reason.com/archives/2008/10/06/who-killed-real-id>
- Weintraub, J.A., & Kumar, K. (1997). *Public and private in thought and practice: Perspectives on a grand dichotomy*. Chicago: University of Chicago Press.
- Western RFID companies flock to China. (2008, February 27). [Electronic version]. *Printed Electronics World*. Retrieved 5/24/2009 from [http://www.printedelectronicsworld.com/articles/western\\_rfid\\_companies\\_flock\\_to\\_china\\_00000835.asp?sessionid=1](http://www.printedelectronicsworld.com/articles/western_rfid_companies_flock_to_china_00000835.asp?sessionid=1)
- What were China's 450 million mobile users 'Searching' for in 2006? (2007, January 18). Press release. Retrieved 2/2/2009 from [http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/01-18-2007/0004508272&EDATE=.](http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/01-18-2007/0004508272&EDATE=)

- Westin, A. F. (1967). *Privacy and freedom* (1st ed.). New York: Atheneum.
- Winner, L. (1978). *Autonomous technology: Technics-out-of-control as a theme in political thought* (1st pbk. ed.). Cambridge, Mass.: MIT Press.
- Wolf, N. (2007). *The end of America: Letter of warning to a young patriot*. White River Junction, Vt.: Chelsea Green Pub.
- Wrong, D. H. (1970). *Max Weber*. Englewood Cliffs, N.J.: Prentice-Hall.
- Wu, P. (2006). New Chinese email spam rules will cleanse the marketplace. Retrieved 2/23, 2008 from <http://www.chinatechnews.com/2006/03/20/3607-new-chinese-email-spam-rules-will-cleanse-the-marketplace/>
- X-files.(1998, February 14). *The Economist*, 346(8055) 39.
- Xinjiang police tightens security checks.(2008, August 5). *Xinhua General News Service*.
- Yin, R. K. (1984). *Case study research: Design and methods*. Beverly Hills, Calif.: Sage Publications.
- York, G. (2005, June 23). Smile! you're on communist camera. *Globe and Mail*.
- Zarrow, P. (2002). The origins of modern Chinese concepts of privacy: Notes on social structure and moral discourse. In B. S. McDougall, & A. Hansson (Eds.) *Chinese Concepts of Privacy*, (pp. 121). Netherlands; Boston: Brill.
- Zarsky, T. Z. (2002-2003). Mine your own business: Making the case for the implications of the data mining of personal information in the forum of public opinion. *Yale JL & Tech*, 5.
- Zetter, K. (2006, June 21). Is the NSA spying on U.S. internet traffic? *Salon Magazine*.
- Zhang, F. (2008, June 25). Number of china's credit card holders doubles in quarter. [Electronic version]. *ShanghaiDaily.com*. Retrieved 7/12/09 from [http://www.shanghaidaily.com/sp/article/2008/200806/20080625/article\\_364455.htm](http://www.shanghaidaily.com/sp/article/2008/200806/20080625/article_364455.htm)
- Zhang, J. (2002). A critical review of the development of Chinese e-government. *Perspectives*, 3(7). Retrieved January 18, 2008 from [http://www.oycf.org/oycfold/httpdocs/Perspectives2/19\\_123102/eGovernment.htm](http://www.oycf.org/oycfold/httpdocs/Perspectives2/19_123102/eGovernment.htm)



Zhao, L. (2006, October 31). The real-name blogger registration system. [Electronic version].

*Southern Weekend*. Retrieved August 10, 2007 from

[http://zoniaeuropa.com/20061106\\_1.htm](http://zoniaeuropa.com/20061106_1.htm)