February 2009

Surveillance and Privacy

Michael Karl Walter-Echols
Worcester Polytechnic Institute

Sequence Number: FJL-LAK1

Panopticon – Surveillance and Privacy in the Internet Age

February 27, 2009

Michael Walter-Echols

Approved:

F. J. Looft, Professor and Head
Electrical and Computer Engineering

An Interactive Qualifying Project Report
submitted to the Faculty of
WORCESTER POLYTECHNIC INSTITUTE
in partial fulfillment of the requirements for the
Degree of Bachelor of Science

Abstract

The right to privacy has been central to democratic society since its inception. In turbulent times, the desire for enhanced national security is often seen to trump an individual's right to privacy. Along with laws permitting expanded government control over the lives of its people, technology has increased the potential for surveillance of the average citizen. This project reviews the concept of privacy rights and the history of privacy. Secondly, it examines the changes to privacy rights that have occurred due to recent events, and evaluate if any significant enhancement to security is thereby achieved. Finally, it provides recommendations on how personal and public security can be enhanced while remaining sensitive to privacy considerations.

Table of Contents

Abstract....2
Chapter 1: Introduction....5
Introduction....5
Impact of Technology....5
Definition of Terms....6
What is Privacy?....6
What is Security?....6
Why does privacy matter?....7
Summary....7
Chapter 2: Overview of Privacy Law....9
Privacy and U.S. Law....9
U.S. Constitution....9
Fourth Amendment....9
Fifth Amendment....11
Fourteenth Amendment....11
Tort Law....12
Privacy Act of 1974....13
Health Insurance Portability and Accountability Act....14
Changes to U.S. Privacy Law since September 11, 2001....14
USA PATRIOT Act....14
FISA and Telecom Immunity....15
Privacy and European Law....15
European Convention on Human Rights....15
European Directive on Data Protection....16
Chapter 3: Development of Surveillance Technology....19
History....19
Slave Passes....19
Photography....21
Biometrics....22
Digital Surveillance....25
State of the Art....28
Data Mining....29
Total Information Awareness....30
CCTV....31
Wiretapping....32
Data Surveillance: Wiretapping the Internet....33
RFID....36
Conclusion....37
Chapter 4: Present and Future Trends....39
The Value of Information....39
Present Trends....39
Social Control....40
Marketing....41
Social Networking....42

Google....43
Projected Developments....44
Private....44
Commercial....45
Political....45
Conclusion....46
Chapter 5: Recommendations and Conclusion....47
Introduction....47
Public Policy....47
Constitutional Amendment for Privacy....47
Private Actions....48
Encryption Everywhere....48
Conclusion....49
References....51

1. Introduction

Introduction

The principles laid down... affect the very essence of constitutional liberty and security. ...They apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property...

Associate Justice Joseph P. Bradley, *Boyd v. United States* (1886)

The right to privacy has been a cornerstone of free, democratic society since its inception. While not explicitly mentioned in the US Constitution, numerous court cases have affirmed that free citizens have a right against government intrusion into their lives emanating[1] from the Fourth, Fifth, and Fourteenth Constitutional Amendments. Indeed, it is difficult to imagine how one might achieve "Life, Liberty, and the pursuit of Happiness"[1] without it. Nevertheless, the right to privacy frequently finds itself in opposition to another unalienable right: the right to security.

Particularly in times of violence and turmoil, the desire for enhanced national security is often seen to trump an individual's right to personal privacy. Although the courts have struggled to balance the right to privacy against other personal and state interests for decades, if not centuries, the aftermath of the attacks of September 11th, 2001 may have tipped the balance toward national security. "If you've done nothing wrong, then you have nothing to hide" is the invariable justification for trading privacy for security. In truth, without privacy for all, there will be security for none: "Those who would give up essential liberty to purchase a little temporary safety, deserve neither liberty nor safety."[2]

Impact of Technology

Concurrent to the enactment of laws permitting expanded government control over the lives of its people, technological developments have exponentially increased the potential for surveillance of the average citizen. With the advent of satellite photography, long-range directional microphones and wireless listening devices, closed-circuit television cameras, and Internet data mining, the potential for an omniscient, omnipotent government presence such as that depicted in George Orwell's *1984* has never been greater. Coupled with the public's complacent attitude towards personal privacy, we may

1 *United States Declaration of Independence*, http://www.archives.gov/exhibits/charters/declaration_transcript.html
2 Commonly attributed to Benjamin Franklin, but this attribution may be disputed. http://en.wikiquote.org/wiki/Benjamin_Franklin

soon face the panopticon: the all-seeing eye from which nothing is hidden.

Definition of Terms

What is Privacy?

There are possibly as many definitions of privacy as there are people to define it. Prior to any further discussion of privacy and the implications of its loss in free society, a working definition for the purposes of this discussion must be established. One of the common definitions of privacy is "the condition of being concealed or hidden"[3]. While this is to some degree accurate in the discussion of privacy rights, the notion of concealment carries with it the connotation of covering something up, usually a crime. Clearly, the protection of privacy can sometimes aid those who wish to commit a crime, but it is legally protected behavior which I seek to discuss here. As I will later show, criminal activity can be uncovered through other means, without invading privacy.

A better definition of privacy can be found with Merriam-Webster: "freedom from unauthorized intrusion"[4]. The inclusion of the word 'unauthorized' addresses the key point that those seeking to violate privacy are exceeding their mandate under the relevant laws. This is critical to any discussion of privacy rights, because the former definition is frequently cited by those who wish to reduce privacy protections. The purpose of privacy is not to protect those who would commit a crime, but rather to make it a crime to interfere with those people who are exercising their legally protected liberties.

Aside from its basic definition, there are also numerous perspectives on privacy, including philosophical, psychological, sociological, economic, and political[2]. While each view contains subtleties of its particular context, all should be considered in the discussion of privacy rights. Although invasions of privacy are often committed by governments, which makes the act inherently political, it is not only political privacy that is relevant in this context. As information becomes more easily and widely accessible, it may be from the private sphere that the greatest threat to privacy comes.

What is Security?

Generally speaking, any mention of security deals with safety or protection from harm. While this meaning is accurate, it is not precise enough for the purposes of this discussion. In the context of this discussion, it is the security of nations and states that is of particular concern. A more precise description of this narrower meaning of security is "measures taken to guard against espionage or sabotage, crime, attack, or escape"[5]. Specifically, it is the interest of the state to guard itself from external attack and internal weakening. Often this interest in protecting the state from harm finds itself

3 Princeton WordNet, http://wordnet.princeton.edu/perl/webwn?s=privacy
4 Merriam-Webster Online Dictionary, http://www.merriam-webster.com/dictionary/privacy
5 Merriam-Webster Online Dictionary, http://www.merriam-webster.com/dictionary/security

in opposition to the interests of individuals to protect their privacy. The interaction of state and individual interests plays a fundamental role in the reconciliation of privacy and security concerns.

Why does privacy matter?

Centuries ago, privacy was relatively easy to protect. If one wished to do something away from prying eyes, it was accomplished behind closed doors, or under cover of night. If one wished to keep a piece of information secret, one took pains not to disclose it. Generally speaking, a loss of privacy was the result of some action on the part of the subject, and could be avoided through prudence. If one experienced a loss of privacy, one had only oneself to blame.

Recent years have brought rapid technological development. Newspapers, radio, and television made it possible for private individuals to become objects of national interest, raising privacy concerns. The telephone made it possible for an individual to project his presence into another's home without leaving his own, raising further privacy implications. However, it is the advent of the digital computer and especially computer networks that have highlighted the necessity in protecting privacy in the modern age.

Once private data is released, it can spread across networks, literally at the speed of light, with no action required on the part of the data's owner. Furthermore, it is increasingly our data, not our physical selves, which determine our actions in the information economy. Our data decides if we have enough money in our bank accounts, if we will be approved for a loan, or how much our car or health insurance premiums cost. If our data can be copied, manipulated, or destroyed without our action or even knowledge, then the same happens to our very identities. When our information is traded and sold to the highest bidder, we lose control over small pieces of ourselves.

Summary

The purpose of this project is threefold. First, I will review the concept of privacy rights and the history of privacy juxtaposed to personal and state security. Second, I will examine the changes to privacy rights that have occurred due to recent events, and evaluate if any significant enhancement to security is thereby achieved. Finally, I will provide recommendations on how personal and public security can be enhanced while remaining sensitive to privacy considerations.

Chapter 1 introduces the concept of privacy rights in the context of security, and why privacy is a relevant concern today. Additionally, a working definition of privacy and security is detailed. Finally, the overall structure of the project is outlined.

Chapter 2 explores the how privacy has evolved in the United States. Beginning with an overview of the laws governing the interaction of privacy rights and the actions of the state, I continue with a description of how these laws have evolved throughout history, especially in response to

technological developments. Furthermore, I will examine how privacy issues are treated in other Western nations, and examine cases that require special consideration.

Chapter 3 examines the history of surveillance and surveillance technology. I will examine how surveillance has been conducted in various nations and points in time, focusing particularly on cases when the surveillance was conducted on a country's own citizens.

Chapter 4 performs an analysis of the current state of surveillance technology and privacy. I will determine the trends which current events are following, and attempt to illustrate what the future may hold if we continue to follow those trends.

Finally, chapter 5 seeks to offer recommendations on how the need for security can be reconciled with the need for privacy.

2. Overview of Privacy Law

Privacy and U.S. Law

U.S. Constitution

The right to privacy is not explicitly guaranteed in the U.S. Constitution. In fact, the word privacy never even appears within the text. Nevertheless, the U.S. Supreme Court has interpreted in certain Constitutional Amendments an implicit right to privacy. This right is seen to be derived primarily from the Fourth Amendment[3], with the Fifth and Fourteenth Amendments also sometimes cited. The court has been clear, however, that such rights are not absolute: other state interests may be more compelling[3]. A brief look at certain key cases reviewed by the High Court will illustrate the legal support for privacy rights within the context of Constitutional Law, as well as where the boundaries of those rights lie.

Fourth Amendment

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.

United States Constitution, Amendment IV

The origins of the Fourth Amendment are found in the "writs of assistance" used by British officers of the Crown during colonial times[3]. These writs were used as "general warrants allowing officers to enter private property and conduct a dragnet search for 'smuggled goods.'"[3] Because officers were not required to declare the object or purpose of the search, the system was easily abused[3], and according to James Otis Jr., placed "the liberty of every man in the hands of every petty officer."[4]

With the abuses of the Crown fresh in the public mind, the Fourth Amendment was drafted to ensure that such acts could not legally continue. Before a police officer can search a person or their effects for evidence of a crime, they must first convince a judge that there is a "reasonable" probability of finding the evidence, and name specifically who or what is to be searched. The corollary to this rule and the basis for the Supreme Court interpretation, is that in absence of such a lawfully acquired

warrant, a person and their property are protected from search: they have a right to privacy.

Naturally, as with all rules, there are exceptions. For example, an officer in "hot pursuit" of a felon is not required to seek a warrant while chasing the alleged criminal: doing so would obviate the need for the warrant, as the target would have long fled by the time he received it[3]. Or, if while executing a lawful search an officer discovers evidence of a new crime "in plain sight", he is not required to turn a blind eye[3]. Typically, such exceptions to the Fourth Amendment are due to simple practicality, and are intuitively obvious. Sometimes, however, it is not immediately clear whether the interests of the government are more compelling than those of the individual. It is these cases, when heard by the Supreme Court, which have defined our understanding of the Constitutional right to privacy.

In one such case, the court outlined a "balancing test" in order to determine whether a search could be considered reasonable. Finding a search to be reasonable under the Fourth Amendment "requires a balancing of the need for the particular search against the invasion of personal rights that the search entails."[5] Thus, even when a search is considered to be an invasion of rights protected under the Fourth Amendment, it may still be considered constitutional as long as the needs of the state outweigh the needs of the individual. For example, when police arrested a man suspected of drunk driving, a blood sample was taken to determine his blood alcohol level. The court found that although the "compulsory administration of a blood test... plainly involves the broadly conceived reach of a search and seizure under the Fourth Amendment"[6], even without a warrant, the state's necessity of quickly documenting the man's level of intoxication overruled his needs of privacy[6]. Exactly what is protected, and how much protection it can be afforded is ultimately decided on a case-by-case basis.

Similarly, the need for "probable cause" has also been abridged by the Supreme Court. In *Terry v. Ohio*, an officer pursued men he suspected of planning a robbery. Believing them to be armed, the officer searched the men for weapons by patting down the outside of the men's clothes, now called a "Terry pat", and discovered a concealed handgun on one of them. When the search was challenged, the court held that the search was constitutional, and that "probable cause" was not required in this case, but rather that "a reasonably prudent man in the circumstances would be warranted in the belief that his safety or that of others was in danger"[7]. This test is referred to as "reasonable suspicion", and is considered a valid justification for a search, even when "probable cause" may not be proved.

In response to the practical needs of law enforcement to act quickly and decisively, the courts appear to be continually expanding state privilege. In fact, the Supreme Court has frequently referred to its "preference" rather than "requirement" for warrants: "the Court has expressed a preference for the use of arrest warrants when feasible... it has never invalidated an arrest warrant supported by probable cause solely because the officers failed to secure a warrant."[8] When combined with the relaxed requirements for conducting a search using "reasonable suspicion", it is arguable that it has become

significantly easier to arrest someone, first by searching them based on "reasonable suspicion", then arresting them by citing the results of the search as "probable cause" – all without a warrant.

Fifth Amendment

...nor shall [any person] be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law...

United States Constitution, Amendment V

Although not frequently cited in privacy cases, the Fifth Amendment serves an important role in the protection of privacy rights, if only as a backup for the rights afforded by the Fourth Amendment. While an individual's private property is protected from illegal searches, the value of such protection is greatly reduced if the suspect himself can be compelled to provide information which aids his own prosecution.

Derived from measures against torture in English law[6], the Fifth Amendment affords the accused the right to refuse to respond to any question if they believe the answer would incriminate them. The law provides protection under a wide variety of conditions, including during trial, regardless if the proceedings are criminal or civil[9], or taking place in Federal or State court[10]. In keeping with its historical precedent, the law also protects suspects under "custodial interrogation" from physical torture[11] by rendering as inadmissible any testimony coerced by physical violence or under any "unfair and inherently coercive context"[12].

Although the protections provided by the Amendment are generally quite broad, the Supreme Court has elaborated on two notable exceptions to "pleading the Fifth". First, the law may not be used to refuse to file a tax return[13], and evidence of criminal activity described in a tax return is admissible in court[14]. Second, the Court held that the Constitution does not articulate a right to refuse to give one's name to police[15], although this is permitted in some states.

Fourteenth Amendment

...No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws...

United States Constitution, Amendment XIV

6 Presented to English Parliament in 1647 as a petition by The Levellers titled *The Humble Petition of Many Thousands*

Passed following the Civil War, the Fourteenth Amendment was originally envisioned to provide Federal protection for the rights of newly freed slaves. Since its passage, particularly during the latter half of the 20th century, the word "liberty" has been broadly interpreted to include a number of implicit rights, including privacy. However, on the role of the Supreme Court justices and their flexibility in interpreting the Constitution, the Court is bitterly divided[3].

At the heart of the legal debate concerning the scope of Fourteenth Amendment protections is how strictly the legislation is to be interpreted. On one hand, some Supreme Court justices take a very strict view of the Due Process Clause of the Fourteenth Amendment. These judges find that "the 'liberty' protected by the clause includes only those rights specifically listed in the Bill of Rights."[3] The role of the Court, they feel, is strictly to interpret the Constitution, and "the proper way to constitutionally protect rights not mentioned in the Bill of Rights is for Americans to amend the Constitution, not for judges to simply interpret them into existence."[3] This view is referred to as procedural due process. On the other hand, other justices feel that interpreting "liberty" is precisely the role of the Supreme Court, and because the justices do not need to seek reelection, they are crucial in safeguarding individual rights[3]. This is known as a substantive view of due process.

During the early years of the Amendment, the Supreme Court based many of its decisions on the stricter procedural view. The Court repeatedly found in favor of reduced state interference in a series of cases, striking down laws imposing maximum working hours in 1905[16] and minimum wage in 1923[17]. However, by 1937[18], and possibly due to pressure from President Franklin D. Roosevelt in support of his New Deal, the Court began to take a more substantive view of due process. One of the most powerful legal precedents supporting a right to privacy came with the decision of *Griswold v. Connecticut* in 1965. Although the subject of the case dealt with abortion and contraception, the legal support for the decision derived from a general right to marital privacy to be found in "emanations" and "penumbras" of the Constitution and its Amendments[1]. Likewise, in a similar case, unmarried people were also found to possess a right to privacy[19]. Thus, the door was opened for the Supreme Court to declare the existence of a general right to privacy.

Tort Law

Another area of U.S. law where a right to privacy is generally recognized is tort law. Whereas constitutional privacy protections are Federal law, and thus effective nationwide, torts are violations of state laws, and therefore vary from state to state. However, Federal law only protects individuals from government action; it is not applicable in disputes between private citizens. When seeking redress for an invasion of privacy perpetrated by a neighbor, shopkeeper, or newspaper, it is tort law which must be called upon.

During the late 19th and early 20th centuries while the legal right to privacy was in its infancy,

the laws were recognized inconsistently, and only as "invasion of privacy"[3]. In 1960, an article by legal scholar Dean William Prosser argued that the tort generally referred to as "invasion of privacy" was actually four distinct torts[3]. Although laws vary between states, most states recognize some variation of these torts:

> *Intrusion: Intruding (physically or otherwise) upon the solitude of another in a highly offensive manner. For example, a woman sick in the hospital with a rare disease refuses a reporter's request for a photograph and interview. The reporter photographs her anyway, over her objection.*
>
> *Private facts: Publicizing highly offensive private information about someone which is not of legitimate concern to the public. For example, photographs of an undistinguished and wholly private hardware merchant carrying on an adulterous affair in a hotel room are published in a magazine.*
>
> *False light: Publicizing a highly offensive and false impression of another. For example, a taxi driver's photograph is used to illustrate a newspaper article on cabdrivers who cheat the public when the driver in the photo is not, in fact, a cheat.*
>
> *Appropriation: Using another's name or likeness for some advantage without the other's consent. For example, a photograph of a famous actress is used without her consent.*[3]

These privacy torts, like most laws, carry with them a number of exceptions. Most notably is an exception for "newsworthiness" which is particularly applicable to *intrusion* and *private facts*: in cases where the media is accused of violating the privacy of private citizens, the courts frequently find that public interest in the facts of a story trumps the individual's right to privacy[3]. This has the side effect of making it very difficult for celebrities and others in the public eye to successfully sue the media for privacy invasions[3].

Another barrier to a successful civil privacy suit is the interpretation of "highly offensive". Because the term must be interpreted by the judge in each case, it is not always clear whether one person's view of what is offensive is shared by the court. For example, in *Miller v. NBC*, a television crew riding with an ambulance filmed a man's death. While the man's wife found this behavior offensive, the television crew manager considered it simply a normal aspect of his job[3].

Privacy Act of 1974

Very little formal legislation on privacy exists at the Federal level. One of the few such pieces of legislation is the Privacy Act of 1974. Enacted following the disclosure of privacy abuses by the Nixon administration, the law restricts the release of private information by government agencies. The records of individuals held by a government agency may be used only for the purpose it was collected, disclosed to law enforcement by written request, or used for statistical purposes in a manner which does not personally identify the individual. Otherwise, the law states that any disclosure, including to another government agency, must be authorized in writing by the individual documented by the record.

Both civil and criminal penalties are detailed for violations[20].

In 2007, the Department of Homeland Security was granted exemptions to the Privacy Act for the Arrival and Departure System (ADIS) and Automated Targeting System (ATS)[21]. Both systems use Passenger Name Records (PNR), data gathered by automated booking systems for airlines. These exemptions are notable especially because the data must often cross international borders, and may result in a conflict between nations which protect data privacy differently. Additionally, because the Privacy Act only applies to records of U.S. citizens or resident aliens[20], foreign nationals have no rights to the data gathered about them using these systems.

Health Insurance Portability and Accountability Act

Another noteworthy piece of Federal data privacy legislation is the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Like the Privacy Act, the purpose of the legislation is to limit disclosures of personally identifiable information, in this case within the health care industry. All health care providers, as well as most health insurers are covered under the Act. The law lists numerous conditions where disclosure is permitted, including for treatment and payment purposes, law enforcement needs, cases of abuse or neglect, and research purposes. In cases where disclosure is not specifically authorized, such authorization must be obtained in writing from the patient. Additionally, disclosures covered by the Act must be the minimum information necessary for the use. Both civil and criminal penalties are outlined for violators[22].

Changes to U.S. Privacy Law since September 11, 2001

USA PATRIOT Act

In the days and weeks following the attacks of September 11th, 2001, while the United States was reeling from the impact of the events, there was a great amount of discussion about the failures in policy and administration which opened the window for the attacks to occur. One of the frequent arguments in the public discussion was that the law enforcement and intelligence communities lacked the freedom to perform their duties effectively because of restrictions placed on them by overly-burdensome civil liberties laws. Congress, eager to show action towards correcting this perceived problem, passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, and introduced a number of changes to privacy legislation in the U.S., including alterations to surveillance, judicial process, and immigration law.

Many of the clauses which are controversial for privacy activists are found in Title II of the Act, which “amends the Federal criminal code to authorize the interception of wire, oral, and electronic

communications for the production of evidence"[23] of terrorism and computer fraud and abuse offenses. One of the clauses extends the ability for the FBI to perform "roving wiretaps"[23], which allows a single court order to authorize surveillance of any device used by a suspect. This has the consequence that an innocent person who coincidentally uses the same phone as a suspect may be subject to surveillance. Also, the Act allows the FBI to apply for a court order to require the "production of certain business records for foreign intelligence and international terrorism investigations."[23] This enables the FBI to compel evidence from third parties, including library reading lists, medical records, and financial information without establishing probable cause or reasonable suspicion – the agency must only assert that the information pertains to a terrorism investigation. The Act also expanded jurisdiction to allow search warrants to be served nationwide[23]. It is feared that this jurisdictional change will allow agencies to select a court district (and judge) which is inclined to approve the order, rather than need to convince a potentially skeptical judge[24, p. 201]. Finally, a section of Title II included the authorization for "sneak and peek" searches, which are served without the suspect being present or notified[23].

A number of sections of the PATRIOT Act found in other titles have also been criticized for damaging fundamental rights. For example, the Act allows for the indefinite detention of immigrants accused of terrorism[23]. Furthermore, the Act greatly expanded the use of National Security Letters (NSLs), which are a type of administrative subpoena. Unlike warrants or other subpoenas, NSLs do not require judicial review. Also, the NSL contains a "gag order," and the recipient is bound from disclosing that the letter was even issued[23].

FISA and Telecom Immunity

In July 2008, President Bush signed the FISA Amendments Act, which broadened the powers of the National Security Agency to conduct communications surveillance[25]. A particularly controversial portion of the legislation granted retroactive immunity from civil lawsuits to communications providers who cooperated with the potentially unconstitutional surveillance program. The law represents an especially disturbing development for privacy rights. By removing any penalties for violating the privacy rights of customers, service providers are encouraged to comply with government requests for access, even if such requests are illegal. The legality of the surveillance program was challenged by the American Civil Liberties Union (ACLU), but the Supreme Court declined to hear the case[26].

Privacy and European Law

European Convention on Human Rights

1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

European Convention on Human Rights, Article 8

In contrast to the U.S. implementation, where privacy protections are inferred from other wording in the Constitution, privacy protections are explicitly laid out in legislation of the Council of Europe. The European Convention on Human Rights, which forms the legal foundation of the Council, details the basic rights and freedoms recognized by the European Court of Human Rights. All member states are party to the convention, and the Court's rulings are legally binding[27].

The purpose of the Convention is to limit interference with personal privacy by the state. Privacy concerns raised in private and commercial contexts are covered by other legislation. The Court permits state interference with an individual's privacy only when specific conditions are met. The privacy abridgment must be in accordance with the law, must pursue a legitimate goal, and must be necessary for the functioning of a democratic society[27].

A unique and interesting feature of the European Court of Human Rights is that it permits individuals to bring their cases to the Court. This makes it possible for individuals to bring their cases directly to the supranational Court, rather than waiting for them to be forwarded onward by their own national courts[27].

European Directive on Data Protection

...data-processing systems are designed to serve man... they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals...

European Directive on Data Privacy

Whereas the European Convention on Human Rights limits privacy violations by government bodies, it was not intended to govern the private sector. Recognizing the need for consistent handling of personal data throughout the EU, Directive 95/46/EC on the protection of personal data was introduced as an overarching regulation on the commercial use of private information. The Directive seeks to implement the recommendations set forth in 1980 by the Organization for Economic

Cooperation and Development (OECD) "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data." The OECD guidelines outlined seven principles to govern the flow of personal data:

> *Data Quality Principle... Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.*
>
> *Purpose Specification Principle... The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.*
>
> *Use Limitation Principle... Personal data should not be disclosed, made available or otherwise used for purposes other than those specified... except... with the consent of the data subject; or... by the authority of law.*
>
> *Security Safeguards Principle... Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.*
>
> *Openness Principle... There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.*
>
> *Individual Participation Principle... An individual should have the right... to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him... to be given reasons if a request... is denied, and to be able to challenge such denial; and... to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.*
>
> *Accountability Principle... A data controller should be accountable for complying with measures which give effect to the principles stated above.[28]*

Guided by the OECD principles, the Directive articulates the rights held by the data subject (the individual whose information is being used) and the responsibilities of the data controller (the entity which is collecting or using the information). The Directive applies whenever a data subject is asked to disclose personal information. The data controller is required to announce what the information is needed for, and is limited to requesting only the data directly required for that purpose. The data may be used only if the subject has explicitly consented. If the controller wishes to disclose personal data to a third party, consent must likewise be granted. Furthermore, the data may only be stored for as long as is necessary to fulfill its function. As a general principle, data deemed sensitive (pertaining to race, sexual preference, etc.) may not be processed, except with explicit consent of the subject or to comply with a law enforcement request[29].

In addition to the right to limit the use and disclosure of personal information, the data subject also has certain rights to the data while still held by the controller. The subject has the right to discover exactly what information about them, if any, a controller holds. If the subject can show that the information is incorrect, out of date, or was illegally acquired, the controller is required to correct or erase it. The controller is also required to disclose the logic upon which automated decisions using personal data are based[29].

EU directives do not hold the force of law. Rather, each member state is required to comply with directives by translating it into laws within their own legal framework. However, states which fail to comply with directives can have actions brought against them to compel them to comply.

3. Development of Surveillance Technology

History

Slave Passes

It should be remembered that no slave was allowed to be off the plantation after sunset, without a written pass.

Allen Parker, *Recollections of Slavery Times*

The beginnings of modern surveillance systems can be readily seen in the development of the slave pass system during the first two centuries of American history. Although no longer in use, the system illustrates the basic components of any surveillance system, including those currently in operation today. More importantly, it demonstrates the ultimate purpose of all such systems: not merely identification and monitoring, but self-policing.

The slave pass relied on a simple rule: no slave was permitted to be away from his plantation after dark without pass from his master. Plantation owners had numerous reasons for wishing to limit the movement of their slaves. One such reason was simple productivity: a well-rested slave could perform more work. Upon arrival in America, families of slaves were frequently split apart, each member being sold to a different plantation. Thus, there was a strong desire on the part of the slaves to visit each other during the night[24, pp. 14-16].

The first level of surveillance which the slaves were subject to was at the plantation level. Considering slaves to be no different from other property, plantation owners frequently maintained lists of their inventory, including lands, tools, animals, and people. Owners monitored the productivity of the slaves constantly. George Washington, writing about a worker at Mount Vernon, complained "last week Caroline (without being sick) made only five [shirts]."[24, p. 15] The demand for closely monitoring the workforce was great enough that by the 1840s, publishers were producing management ledgers, such as "The Cotton Plantation Record and Account Book, No. 1 Suitable for a Force of 40 Hands or Under."

Of greater concern than mere productivity, however, was the threat of rebellion. Slave mobility was the foundation of communication between groups of slaves on various plantations. In addition to the exchange of news, slave mobility also permitted the transportation, stockpiling, and trade of weapons and supplies, which were frequently stolen. By restricting the movement of slaves between plantations, landowners limited the slaves' ability to resist, and encouraged compliance[24, pp. 14-16].

If a plantation owner needed to send his slave on business to a nearby town, he would write a handwritten note, or pass, stating that the slave had his permission to travel. Typically, such passes merely identified the slave by name, where he was going, and the period of time for which it was valid. For example, this pass from Missouri:

Gentilmen let the Boy Barney pass and repass from the first of june till the 4

To Columbas MO for this date 1852

Samuel Grove[24, p. 19]

The first pass laws were enacted in Virginia in 1642. Interestingly, these first laws targeted poor white indentured servants, rather than slaves. Anyone wishing to leave the colony was required to carry a letter from the governor certifying that he was neither a fugitive nor a debtor. Conversely, in 1656 a law was passed requiring Native Americans who wished to trade within the colony to acquire a pass or "ticket." It was not until 1680 that the first slave pass law was enacted in Virginia. Other states soon followed suit[24, p. 19].

The pass system was enforced by slave patrols. Slave patrols represented an early predecessor to the modern police force, tasked with the functions of surveillance and corporal punishment. A patrol consisted of a group of three to ten armed white men who rode from plantation to plantation, searching "for runaways, weapons, or supply caches that might indicate escape plans."[24, p. 17] Any black person found without a pass was flogged and returned to his plantation, often in return for a bounty. The random nature of the patrols ensured that they were constantly feared by slaves, who were compelled to self-policing caution, lest they be punished.

For the slave pass to be effective, it was crucial that slaves remained illiterate. Any slave who learned to read and write could easily write a pass for himself or others. He became the "antebellum hacker, the information outlaw, who could crack the code of the planters' security system."[24, p. 20] To prevent this, numerous states passed laws outlawing the teaching of slaves. Often, the patrollers were themselves often unable to read. Slaves, knowing this, could pass off any random letter as a note from their master, and "the captain would take it, look it over wisely, then hand it back telling the slave to go."[24, p. 21]

In order to combat the counterfeiting of passes, technology was employed. By 1783, several southern cities were issuing slaves badges made of tin or brass. On each was stamped the slave's occupation, the date, and a number to record payment of the annual slave tax.[24, p. 25] In these badges we see possibly the first numbered IDs in America. Manumission papers were also a popular target for forgery by literate slaves. This was made vastly more difficult by 1844, when they began to be printed on standardized forms.[24, p. 27]

By the time of the Civil War, the pass system was no longer used solely to restrict the movements of slaves, but was instituted to control the travel of both Union and Confederate soldiers. Often printed as standardized forms with blanks to be filled in by hand, these passes included a list of physically identifiable features we are familiar with today, including age, height, weight, eye and hair color, and distinctive marks in addition to the subject's name. To combat forgery, the passes were frequently printed using a jumble of different fonts.[24, pp. 30-31]

With the emancipation of the slaves following the Civil War, the slave pass system had lost its purpose. However, this was hardly the last time a broad system of identification, monitoring, and control was instituted in the United States. The history of the slave passes teaches a number of lessons in surveillance, both in its application and its circumvention.

Photography

During the early 1800s, the population of American urban centers exploded. Between 1800 and 1860 New York's population grew from 60,000 to one million[24, p. 34]. In an attempt to control social unrest and bring order to the growing chaos of the cities, professional police forces were established, beginning with London in 1829[24, p. 35]. By 1845, New York had America's first full-time, armed police force. With mass immigration and urbanization, these new police officers faced a city full of strangers, and found the old tools of physical descriptions and wanted posters insufficient. Local governments were clamoring for better forms of identification to mark and control criminal elements[24, p. 36].

Meanwhile, in 1839 Louis Jacques Mande Daguerre and Joseph Nicephore Niécpe invented the art of rendering photographs onto glass plates using a 20 minute exposure: the "daguerreotype" was born[24, pp. 36-37]. As the technology improved and exposure time was reduced, photographic portraits became wildly popular with the expanding middle class. In 1841, cheap, quick paper prints became available, and by 1853, Americans were buying nearly 3 million daguerreotypes each year[24, p. 37].

Since the early 19th century, many courts had begun keeping permanent paper records with details and descriptions of defendants and prisoners[24, p. 37]. Police departments in the UK shared bulletins containing physical descriptions of wanted persons, and many police in England and France held weekly parades of prisoners, so that officers from neighboring jurisdictions might locate wanted persons[24, pp. 37-38]. In 1841, police in France added routine photographing to their system of processing prisoners, and in 1842, police in Britain followed suit[24, p. 38]. By 1853, the practice had spread to New York, where the NYPD began photographing repeat offenders and publishing them in "rogues' galleries," where the public was "invited to call and examine."[*ibid* This practice had the dual function of identifying wanted lawbreakers, while also enrolling the middle class into the police

surveillance apparatus[24, p. 38]. Likewise, by the 1870s, police in San Fransisco were carrying "mug books" with photos of criminals to help aid the memory of people questioned on the street. Like the rogues' galleries, this practice helped to create a mentality of "insider" and "outsider" classes[24, pp. 38-39].

With the growing popularity of photography in law enforcement circles came logistical problems: how was the growing collection of photographs, physical descriptions, lists of distinguishing marks, and dates of offenses to be cataloged? Attempts were made to index by name, physical description, numerical code, and date, but all proved unwieldy and time-consuming[24, pp. 39-40]. Without an effective organizational system, the efficacy of these records as police tools was greatly diminished[24, pp. 41-42].

Biometrics

In effort to objectively and accurately index police files, a young Parisian police clerk by the name of Alphonse Bertillon created a system of eleven precise anthropological measurements to identify individuals. By taking the measurements using metal calipers and following precise scientific methodology, it was possible to build an exact, reproducible statistical portrait of a prisoner. Dubbed Bertillonage, his system entered service in the late 1870s, and quickly found wide usage. Because of their accuracy, these measurements were often preferred over the photographs they were intended to index[24, p. 44].

Now, each prisoner had a card in police dossiers which included mug shots, a description of physical appearance, distinguishing marks, and Bertillonage measurements. Because Bertillonage provided concise numerical results, measurements could be telegraphed to other jurisdictions, permitting prompt and accurate identification, even over large distances. By the 1890s, Bertillonage was in use by police departments worldwide. In reaction to the rising anarchist movement of the era, political radicals soon joined common outlaws in police identification files[24, pp. 44-45].

To produce accurate results, the person taking the measurements, known as a Bertillon operator, was required to follow a strict methodology[24, pp. 44-45]. Unfortunately, to save time and effort, police forces often simplified their measurement techniques. The resulting data was often only internally consistent, and lost its value when exchanged with other departments. The resulting patchwork of inconsistent implementations greatly reduced the effectiveness of Bertillonage as a system for identification[24, p. 46].

Around the time that Bertillon was developing his system of measurements, William Herschel, chief administrative officer of the Hoogley district of Bengal, began using inked handprints to verify the identity of contractors, pensioners and other official contacts[24, p. 47]. Meanwhile, Francis Galton studied fingerprints, developing a classification system of loops, whorls, and arches. Later, this

system was further refined by Edward Henry by counting papillary ridges. In a letter to the journal *Nature* in 1880, physician Henry Faulds suggested dactyloscopy, or fingerprinting, as a method for criminal identification[24, p. 48].

Early on, fingerprinting was seen as a way to overcome the homogenizing effects of race. In 1902, one expert on identification noted that dactyloscopy helped "in the official identification of Chinese, Negroes, and other races the features of which at least to the Caucasian eye, offer hardly sufficient individuality to be at all times trustworthy."[24, p. 49] "In the United States, the first populations to be fingerprinted en masse were convicts, petty criminals, soldiers, and Native peoples."[*ibid*]

In 1902, Scotland Yard incorporated dactyloscopy into its Bertillonage[24, p. 49], although in general, adoption of the technique was initially slow. One early use in the United States was to stop hired impostors from sitting the exams for New York police applicants[24, pp. 49-50]. Fingerprinting in U.S. police departments began in earnest after a demonstration by Scotland Yard detective John Kenneth Ferris at the 1904 World's Fair in St. Louis. Within a few months, dactyloscopy was in use in Boston, Baltimore, Washington D.C., St. Louis, Cincinnati, Cleveland, Louisville, Indianapolis, and Memphis. Fingerprints were added to the NYPD Bertillonage files in 1906, and in 1907 the Navy employed dactyloscopy to bust deserters[24, p. 50].

Following the World's Fair, the deployment of fingerprinting in law enforcement rapidly expanded, turning into a national institution. The fingerprint files maintained at Leavenworth Penitentiary formed the basis for the National Identification Bureau, which later became the FBI Bureau of Identification[24, p. 50]. Meanwhile, the Commissioner of Indian Affairs of the Department of the Interior began using handprints on the reservations with payment records and land deeds, such as the ones in which the Lakota were "forced to privatize and surrender much of the Rosebud Reservation in 1907."[*ibid*] Nationwide use of dactyloscopy coincided with a major white land grab, and government agents in charge of building dossiers on native people were urged to "use the greatest care in carrying out this plan, as it is desired to have, within the shortest time possible, an infallible method of identification in case of dispute or attempted fraud."[24, p. 51]

1910 saw the first criminal conviction based on fingerprint evidence. "The defendant... was a Black man accused of robbing and killing a white woman."[24, p. 51] The only evidence against house painter Thomas Jennings was a set of prints left in the paint. A *New York Times* article of the time noted that even if Jennings "had left the marks... that is no absolute proof that he committed the murder."[*ibid*] Nevertheless, the conviction, and the death sentence it carried, was upheld by the Supreme Court.

As fingerprinting gained acceptance, the upper classes began calling for identification and

registration of the entire population. In other parts of the world, this had already occurred: by 1900, the entire population of Buenos Aires had their prints and photo on file with the police, military, and Interior Department. Somewhat presciently, by Word War I opinion makers in the US debated fingerprinting all "aliens," and most military applicants by this point were photographed and fingerprinted to prevent deserters from reenlisting[24, pp. 51-52].

Despite the view among the elite that having one's photo and prints on record with the police was "easily tolerable,"[24, p. 52] for many citizens it was seen as "an insulting mark of incrimination,"[*ibid*] a view that fueled popular resistance to dactyloscopy. Growing public distrust of the system is illustrated by the June 1916 case where NYPD officer Frank Rice arrested three teenage boys on charges of "disorderly conduct." The boys had been playing baseball in a neighborhood where office Rice had been ordered to stake out and bust violators. The boys were convicted, fined, and ordered to submit their fingerprints in accordance with a 1913 disorderly conduct statute. The result was public outrage: "the all-American game could now get you jail time and a permanent record?"[*ibid*] In response, the courts refined the definition of offenses which would require fingerprinting to include "jostling... pickpockets... rowdyism... degenerates, beggars, confidence men, swindlers... disorderly women, intoxicated persons and vagrants"[24, p. 53] but not baseball or "ordinary street brawls."

Towards the end of World War I, calls for national registration increased, and took on a more overtly political tone. The far left was greatly opposed to the war, and saw it as a conflict between the rich but fought by the working class. During the latter part of the 1910s, a string of bombings by various anarchist groups raised the profile of the radical labor movement in the country, and fingerprint registration was heralded as a way to control leftist agitators[24, pp. 53-55]. In an attempt to better control the general unrest, a program to "bring about closer co-operation by interchanging finger prints and criminal records"[24, p. 56] between New York and Chicago was instituted in the summer of 1919.

Employers also found dactyloscopy useful as a way to "enforce black lists against radicals by preventing organizers from using multiple identities."[24, p. 56] At two adjacent plants operated by Carnegie Steel, "workers discharged in one plant drifted across the river to the other. They readily found employment until the company finally began fingerprinting applicants. It then was able to detect those who had been discharged or rejected at another plant."[24, p. 57] At another company, only one employee refused to submit to fingerprinting when it was instituted. "Subsequently, the company, which had kept track of him, learned that he had fallen into the toils of the law in connection with a bolshevist meeting raided by police."[*ibid*]

Given the way it was used against them, it should be no surprise that the working class developed a growing resistance to institutionalized dactyloscopy. Opposition from the labor movement and other targeted groups, "such as African American domestic workers and hotel employees – kept

compulsory printing in check. By the late 1920s registration campaigners had shifted their efforts from compulsory to 'voluntary' fingerprinting."[24, p. 58] Foreshadowing the justifications given for increased surveillance 80 years later, "voluntary" fingerprinting was portrayed as a patriotic civic duty by organizations which funded and organized registration efforts, including the US Chamber of Commerce, the American Bankers Association, Daughters of the American Revolution, and the American Legion. "The Boy Scouts signed up en masse – one million in all."[*ibid*]

Finally, the registration efforts reached a crescendo in 1936 in Berkeley, California. Coordinated by the police chief and local businesses, the "goal was to create police print files for the town's entire population."[24, p. 58] Newspapers ran supportive articles while businesses gave "5 percent discounts for citizens who could show merchants their police-issued 'merit cards' stating in bold print 'I have been fingerprinted.'"[24, p. 59] The desire for fingerprint registration was stated plainly by police: it would "bring about the identity of, and enable us to follow the movement and activities of, Communists, Anarchists and Radicals."[*ibid*] The Berkeley registration drive was steeped in an "us" vs. "them" mentality, clearly stating that the surveillance tool was to control the undesirables *du jour*. One of the key organizing groups, the California Junior Chamber of Commerce, professed that "a law should be passed under the terms of which an individual convicted of revolutionary activity should be incarcerated, and continually held in a concentration camp."[*ibid*]

In response to the Berkeley drive and the registration movement in general, in 1938 the ACLU published a pamphlet titled *Thumbs Down!*, which dismantled the arguments for registration and asserted that fingerprinting "provides the basis for a labor blacklist... offers employers an easy means of control over and intimidation of their employees... would curb severely the movement of citizens... would be intended as a whip for the persecution of aliens... [and] subjects the whole populace to police surveillance."[24, p. 59] Similarly, the *New Republic* explained that there "seems no doubt that the instigators of the Berkeley fingerprinting jamboree are in fact people with strong fascist leanings, who hope to use the device against labor and 'radicals' – a term that, to the Pacific Coast's high blood pressure, includes even the mildest liberals."[24, p. 60]

Although no national registration law was ever passed, numerous local laws required fingerprints for various documents, including birth certificates and commercial driver's licenses. Despite the lack of universal registration, through the widespread use of photo identification and fingerprinting the American public became more accustomed to and accepting of routine surveillance. Using the next great advance in technology, the acceptance of routine, ubiquitous surveillance was brought to a new level entirely.

Digital Surveillance

Computing devices have a long history, but one marked by great periods without significant

development. For most of civilization, the abacus in its various forms was the only computing instrument available. It was not until the 17th century that mechanical adding machines were developed by Pascal and Leibnitz, but neither design found particularly widespread use. Two centuries later, Charles Babbage introduced the Difference Engine, a mechanical wonder capable of computing polynomial functions. Like its predecessors, however, it was extremely expensive to produce and found only limited application[24, pp. 79-80].

In the early 1880s, a clerk for the US Census Bureau named Herman Hollerith puzzled over the difficulties involved with performing the decennial census. Inspired by the labor saving devices which revolutionized the agricultural and textile industries, he sought to to similarly use mechanization to solve the census problem. In 1884, Hollerith applied for a patent on a tabulating machine modeled after the power loom[24, pp. 80-82].

The industrial power loom of the 1880s was capable of weaving a variety of patterns by virtue of its ability to be "programmed" with a series of cards punched with holes to represent the desired pattern[24, p. 81]. Using a similar technique, Hollerith's tabulating machine was able to "read" data from a series of cards with holes punched to represent answers to census questions. In combination with high speed mechanical systems, large numbers of cards were able to be sorted quickly. "By 1890 Hollerith's new Tabulating Machine Company was under contract with the Census Bureau to analyze that year's count. Whereas the 1880 Census had asked only five questions and took most of the next decade to tabulate, Hollerith's number-crunching engines processed forms with over two hundred questions, got the job done in a fraction of the normal time, and did it for only two-thirds the standard price."[24, p. 82]

In contrast to the previously conceived machines, the Hollerith machine was both affordable (at least to governments and large corporations) and politically useful. The speed with which results could be analyzed allowed the state to understand its citizens at a level of detail previously unimaginable. Using the tabulating machine, "government agencies could search census data for all employed women, or unemployed men, or draft age men, or whatever else might be worth knowing. If properly applied, the new technology would revolutionize the census and render the American population more transparent, more useful, and ultimately more governable."[24, p. 82]

The usefulness of the machines was not unique to America, and governments around the world were eager to lease the tabulating machines. Naturally, Hollerith's company, known since 1924 as International Business Machines, was equally eager to profit from the demand. By the early 1930s, the National Socialist government of Germany was among IBM's customers[24, pp. 82-83]. "Immediately after the Nazis took power in January 1933 they set about redesigning the national census, transforming it from a muted, generalized profile of the people and the economy into a demographically exact instrument for focusing on and targeting sub-populations... So the Nazis contracted with IBM through

the firm's German subsidiary, Dehomag (short for Deutsche Hollerith Maschinen Gesellschaft)."[24, p. 83]

It is unclear exactly to what degree IBM was aware of the ultimate purpose of the Nazi government's data processing project. However, it is clear that the new technology furnished the regime with a highly detailed profile of the population. The tabulating machines, which now used "new cards, with space for eighty variables, created *super detailed* population profiles that allowed the Nazis to identify not just Jews, but even select subsets of Jews... The first to go were wealthy Jews of Eastern European extraction, who as rich 'outsiders' were easily targeted."[24, p. 83] While the previous surveillance technologies like fingerprinting and Bertillonage enabled governments to keep track of known enemies, the new data processing technology gave them the capability to identify new ones.

The tabulating machines were employed at every large operation which needed to track large data sets, such as war industries and slave labor camps. "All factories and work camps had Hollerith machines for selecting the type and amount of labor needed, directing supplies, managing accounts, and compiling reports."[24, p. 84] Most chillingly, "the infamous ID numbers tattooed on concentration camp inmates' forearms correlated to each prisoner's Hollerith card and the census data it contained: the tattoos were death camp barcodes."[*ibid*] The technology was now available to positively identify, at the individual level, large populations and routinely track a person's movements or any and all data available about them.

Meanwhile, in August 1935, the United States passed the Social Security Act[24, p. 85]. Initially, the law did not require an ID number. However, once the identification requirements became apparent, the law was met with great resistance on both left and right. "GOP heavyweight John D. M. Hamilton attacked Roosevelt's Social Security system as crypto-fascist, claiming that all Americans would be forced to wear metal ID tags. William Randolph Hearst's *New York Journal-American* declared the new pension system... would require workers to wear dog tags 'for the privilege of suffering a pay cut.'"[*ibid*] Likewise, unions worried that the new Social Security numbers would be "hijacked by bosses to track and blacklist organizers"[*ibid*] and insisted on the ability to replace numbers when demonstrating cause.

History shows that many of these concerns had merit. In 1939, the "function creep" began when J. Edgar Hoover persuaded Roosevelt to issue an executive order giving the FBI access to Social Security files in any federal criminal investigation[24, p. 86]. Indeed, the Social Security system became a valuable stockpile of information. By 1945, the Social Security Administration's punch card files occupied six acres of storage[*ibid*]. Yet even such a volume of data remained manageable with improvements in technology: in 1956, the Administration upgraded to the new IBM 705 vacuum-tube electronic computer[*ibid*].

While governments were improving their data processing abilities with the new technology, commercial interests were taking advantage as well. However, the shift to digital technology presented a problem to companies which indexed their records by name and address. The new machines were unable to cope with inconsistencies and redundancies as humans were, and these limitations were exploited by individuals seeking to escape debt or criminal records. Like the Social Security Administration, corporate entities also needed a numerical ID by which to manage their records[24, pp. 86-87].

By the early 1960s, calls for a national ID number by the financial industry were at an all-time high. Nevertheless, the libertarian spirit of Americans ensured that decades of legislative attempts failed. In response, large businesses simply opted to demand disclosure of the Social Security Number from their customers in exchange for services. As the *Harvard Business Review* pointed out, "if an applicant refuses to give his number, the answer is obvious; he doesn't get credit, his check is not honored, or his insurance application is rejected."[24, p. 87] Meanwhile, the tax code was also amended to allow the Internal Revenue Service to begin using the Social Security Number as an individual taxpayer ID[30].

Now, with everything from government agencies to large financial corporations using the Social Security Number as a national identification for every individual, great swaths of unconnected personal information could be collated and linked with a unique, machine-friendly number. "One of the most important firewalls in the structure of modern privacy had been quietly demolished. And lest one miss the larger implications here, suturing together disparate financial dossiers is not solely a question of money. Such files can contain information on a subject's residence, employment, and medical history."[24, p. 87]

The simultaneous rise of electronic computers enabled tasks which were previously logistically impossible, like sorting and analyzing hundreds of thousands of individual records for any desired piece of information. When combined with nascent computer networking, large databases of personal information could be transmitted over large distances and combined with others. Each added source of information fills in gaps, painting an increasingly comprehensive picture of each individual, and all without their consent or even knowledge.

State of the Art

It is no coincidence that all modern surveillance techniques depend on computers, networks, or the combination of both. The act of surveillance deals fundamentally with the acquisition, transmission, and analysis of information. Computers are tools designed specifically to replicate and process information as rapidly as possible, and networks transmit it quickly over large distances, and with high fidelity. It should be no surprise then, that computer technology gave birth to the modern

surveillance society.

Data Mining

Data mining is "the application of database technology and techniques (such as statistical analysis and modeling) to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results."[31] Like any statistical analysis method, "data mining by itself is ethically neutral."[32] However, because the purpose of the technique is to predict future events, it runs the risk of negatively impacting targeted subjects when used irresponsibly. It is not so much the act of data mining itself which presents a privacy concern, but rather the nature of the data contained in the database, how it was acquired, and the purpose for which it is used.

The need for data mining is clear and practical one: we are drowning in information. A 2003 study by the University of California at Berkeley found that "print, film, magnetic, and optical storage media produced about 5 exabytes of new information in 2002."[33] To put this staggering volume of data in perspective, "if digitized with full formatting, the seventeen million books in the Library of Congress contain about 136 terabytes of information; five exabytes of information is equivalent in size to the information contained in 37,000 new libraries the size of the Library of Congress book collections."[*ibid*] Furthermore, "ninety-two percent of the new information was stored on magnetic media, mostly in hard disks"[*ibid*], meaning that the information is already digitized and a prime candidate for automated processing. It is important to note that these figures describe *new* data, and do not take into account all the information *already* in databases and filing systems.

In order to perform useful analysis on this mountain of data, it must be processed somehow. However, "the classical approach to data analysis relies fundamentally on one or more analysts becoming intimately familiar with the data and serving as an interface between the data and the users and products."[34] As with many tasks requiring human work, "manual probing of a data set is slow, expensive, and highly subjective."[*ibid*] Unsurprisingly, "as data volumes grow dramatically, this type of manual data analysis is becoming completely impractical in many domains."[*ibid*]

Both the public and private sector make extensive use of data mining. Businesses around the world make use of "database marketing systems, which analyze customer databases to identify different customer groups and forecast their behavior."[34] However, as commercial databases become more detailed and more accurate profiles of customers are built, concern is growing about the "collection of personal information... [and] how the collected information will serve the program's purpose."[35] The U.S. federal government employs data mining for improving service, detecting fraud and waste, analyzing research, managing human resources, and detecting criminal and terrorist activities.[32] While improving the efficiency of all of these processes is laudable, "those using data mining [to predict crime]... must be careful to put in place requirements that detail when action may be

taken against an individual as the result of data mining activities and what is done with mined information that is subsequently determined not to be relevant to an investigation."[35]

The American Statistical Association (ASA) ethical guidelines admonish statisticians to "adhere to appropriate rules for the protection of human subjects, including particularly vulnerable or other special populations who may be subject to special risks or who may not be fully able to protect their own interests."[32] On numerous occasions throughout history, the failure to anticipate how an analysis will be used has ended in tragedy. The roundup of Jews, Roma, Communists, and other such enemies of the Nazi government is an extreme example. Similarly, though far less violently, the data from the U.S. Census Bureau aided in "the round up of the Japanese American population on the West Coast in the months after Pearl Harbor. Reflecting on this experience, former Director Prewitt, remarked, 'In World War II we violated our principles even if we didn't violate the law, and we assured people we wouldn't do it again' (*New York Times* 7/29/2004, p. 19)."[*ibid*] Unfortunately, despite this assurance the same Bureau provided "5 digit zip code data from the 2000 Census on persons of Arab American ancestry to the Department of Homeland Security (DHS)"[*ibid*] which resulted in the arrest or deportation of over 1,200 Arab Americans[36].

Data mining activities also run the risk of producing incorrect results when based upon false assumptions about the data. "The fact that a procedure is automated does not ensure its correctness or appropriateness"[32] reminds the ASA. While false positives must be considered with virtually all attempts at pattern recognition, they are especially problematic when incorrect results directly impact human subjects. For example, consider "the problems encountered by Senator Kennedy of Massachusetts in repeatedly being denied permission to board commercial airlines because his name was on a Transportation Security Administration 'do not fly' list because of concerns about someone else with the same name."[*ibid*] Naturally, being a U.S. Senator, "Kennedy was, with some effort and time, able to resolve the matter. But if you are not Senator Kennedy or some other prominent person with the resources and contacts to get redress, the task of dealing with a 'false match' may not be a simple one."[*ibid*] If the data mining project seeks to identify criminals or terrorists, rather than merely barring entry onto aircraft, the false positive becomes orders of magnitude more damaging.

Total Information Awareness

Perhaps the most ambitious data mining project yet proposed was the Total Information Awareness (TIA) project, which sought to unify various commercial and government databases. Later renamed Terrorism Information Awareness after negative media response, TIA was created under the purview of the Information Awareness Office (IAO), whose mission was to "imagine, develop, apply, integrate, demonstrate and transition information technologies, components and prototype, closed-loop,

information systems that will counter asymmetric threats by achieving *total information awareness*."[7] The purpose of the project was to "pull together all the disparate records of everyday life. From the digital trails of credit cards, electronic tolls, banking transactions, health records, and library use it sought to create one 'virtual, grand database' that could be data-mined for interesting and incriminating patterns. "[24, pp. 202-203]

Public reaction to TIA was swift and negative. The *Washington Post* stated succinctly: "the potential for abuse is enormous."[24, p. 203] *Fortune* magazine elaborated that "every telephone call you make, every credit card transaction, all your e-mail and instant messages, all your medical records, your magazine subscriptions, your police record, driver's license records, gun purchases, travel records, banking records – all would be fed into a hopper and sifted by the TIA spy software."[*ibid*] Arguably, such a system does not merely have the potential for abuse, but is naturally abusive of personal privacy – by making use of records which were created for completely different purposes, and subjecting the entire population to routine surveillance and criminal investigation. Also unhelpful for the project's reception by the public was its head, the "politically radioactive retired Rear Admiral John Poindexter, who was infamously convicted on five felony counts of lying to Congress and destroying official documents during the Iran/Contra Affair (he was later acquitted on technicalities)."[*ibid*]

The public outcry against the TIA project eventually resulted in a congressional audit of the IAO and in 2003 congress defunded the office[24, p. 203]. Despite the officially shutting the project down, a significant portion of the programs continue to be developed by other government agencies. TIA component technologies continue to receive funding, although their use is restricted to military purposes or intelligence against foreigners[37].

CCTV

The closed-circuit television (CCTV) camera is perhaps the most ubiquitous form of routine surveillance encountered in daily life in the industrialized world. The universal presence of these cameras means that most people have become accustomed to their presence, and paradoxically makes them effectively invisible. While individual CCTV installations do present some privacy implications, they have become an accepted and even expected part of everyday life. However, as with most surveillance technologies, the ability to network them transforms these electronic eyes from privacy nuisance to privacy nightmare. Also, the CCTV camera is increasingly leaving the "private and semi-private space to which it was confined from the 1970s till the mid-1980s."[38] The result is that people are more frequently being video monitored in public spaces, often by the local authorities.

Nowhere is the proliferation of CCTV surveillance more evident than the city of London.

7 As the IAO has been shut down and no longer has any official presence, this mission statement is no longer available from an authoritative source. It can still be found verbatim on several other websites, however.

Although an official account is unavailable, it was estimated in 2002 that "Londoners are monitored by at least 500,000 CCTV cameras."[39] When compared to the city's population, "there is approximately one camera for every fourteen people."[*ibid*] So pervasive is this form of routine surveillance, that "in a single day a citizen of London could expect to be 'filmed by over three hundred on over thirty separate CCTV systems'"[*ibid*]. Not only can the camera network observe passersby, but it can speak to them as well. Loudspeakers mounted with the cameras give operators the option of "publicly berating bad behaviour and shaming offenders into acting more responsibly."[40] Additionally, the city is considering installing a microphone linked to an "aggression detector" similar to a system that has been "fitted to CCTV cameras on the streets of Groningen and Rotterdam in the Netherlands. "[41] The technology would "continually analyze the sound in the surrounding area. If aggressive tones are picked up, an alarm signal is automatically sent to the police, who can zoom in the camera to the location of the suspect sound and investigate the situation."[*ibid*]

On their own, the camera systems in London are already invasive. When combined with other systems, however, the power of the system and therefore the threat to privacy is multiplied. The city's traffic cameras are linked to an "automatic number plate recognition system."[39] While the primary function is to check "with a central database to see if the daily [congestion] fee has been paid"[*ibid*], when a vehicle is suspected of being connected to a crime, the system is also capable of tracking the car as it travels and "automatically alerts officers to a vehicle's route across the city."[42]

London is by no means the only major city with a widespread video surveillance system. Numerous American cities are planning or have already deployed camera systems. Assuming it can get the funding, "New York City, specifically lower Manhattan... will have a similar system [to London's] in place by the decade's end."[43] In Washington D.C. an advanced, "centrally monitored, citywide closed-circuit television surveillance system" began construction in 2002.[24, p. 109] When completed, "the Metropolitan Police Department (MPD) plans to operate over 700 cameras, watching streets, schools, Metro stations, federal buildings, and even parts of a Georgetown business improvement district" with the feeds "streamed to the MPD's $7 million, 'NASA-style' Joint Operation Command Center. Filled with video recorders, computers, and communications gear, this room is staffed by the D.C. police, Secret Service, FBI, and at times other agencies."[*ibid*] Perhaps even exceeding the London system in power, this CCTV network "will have the ability to read license plates and track cars moving through the city, zoom in on individuals, read newsprint from hundreds of feet away, and send real-time images to the laptops of the department's one thousand patrol cars."[24, pp. 109-110]

Wiretapping

The practice of surreptitiously listening in to a telephone conversation, commonly referred to as

wiretapping, is one of the forms of surveillance of which the public is most widely aware. Commonly depicted in the popular media in the context of law enforcement or espionage stories, it is conceptually easy to understand: the listener, usually with the cooperation of the local telephone authority, connects to the telephone network so that both sides of a conversation can be heard, often recording the conversation for later analysis and for use as evidence in trial. In fact, the word *wiretap* stems from the (now deprecated) practice of physically attaching clips, or taps, to the telephone wire[44].

While the technology of the telephone was in its infancy, with calls needing to be physically connected by a human switchboard operator who was in a position to listen to the call, the expectation of privacy was relatively low. However, as direct dial and automated switching technology became commonplace, the average telephone user began to expect that each conversation was shared by only themselves and the person to whom they were speaking. When placing a call, the caller was in effect renting a circuit which connected them to the desired party for the duration of the conversation. The courts also recognized this expectation of privacy, and wiretapping was normally permitted only with a court order[45].

Telephone networks have continued to evolve, and now calls are transmitted almost entirely in digital form, with only the final connection between the caller and the local exchange transmitted using the older analog circuits. The bulk of the transmission is carried by a digital data network, which often also carries Internet data. With telephone calls being simply another stream of packets traversing the network, the technical nature of the wiretapping is radically changed. "The Hollywood image of an FBI agent with a pair of alligator clips is a thing of the past"[46], instead, with the click of a mouse the data stream can simply be copied and transmitted or stored anywhere on the Internet, with legal permission representing the only remaining hurdle.

That legal hurdle has been rapidly lowered in response to the advance in technology. Because "lawful intercept in today's world depends on cooperation of the carrier"[46], the 1994 Communications Assistance for Law Enforcement Act (CALEA) required carriers to install equipment to facilitate ease of surveillance by law enforcement[47], and the passing of the USA PATRIOT Act greatly weakened the legal requirements for wiretapping. Strong evidence exists that routine use of wiretaps is rampant: an "internal FBI memo from 2000 that detailed the Bureau's routine and widespread violations of privacy laws"[24, p. 200] lends credence to allegations that the PATRIOT Act was "just a mopping-up operation that legalized already existing and ongoing, yet illegal, forms of investigation."[*ibid*]

Data Surveillance: Wiretapping the Internet

There is virtually no technical difference between wiretapping a modern digital telephone network and performing surveillance on Internet traffic. Both involve making a copy of a stream of

data in transit, and viewing or analyzing it. However, because of the many different types of data transported by the Internet, its surveillance is significantly different, qualitatively speaking. Not only can the interception of Internet data yield voice communications, but also email, instant messaging, financial transactions, and web activities may also be exposed. Also, unlike the older analog telephone lines which connected only two parties at a time, Internet connections can simultaneously support thousands of individuals' data. Because essentially all forms of electronic communications are now at least in part carried by the Internet, surveillance of the Internet is tantamount to the surveillance of all electronic communications.

Legally speaking, the Electronic Communications Privacy Act of 1986 granted data sent by computers the same protections as telephone conversations[48]. Ideally, this means that any attempt to intercept Internet communications must have a search warrant approved by a judge in order to be lawful. However, two important caveats exist which, when exploited, can potentially render all Internet traffic unprotected. First, exceptions to these privacy protections can still be made through other laws; second, the PATRIOT Act lowered the legal standard for electronic surveillance just as it did for the more traditional form[23].

Even despite the legal loopholes built into the system to allow expedient access to protected communications for law enforcement purposes, there is compelling evidence that the U.S. government has nevertheless violated laws protecting the privacy of its citizens. Two separate cases allege that the National Security Agency (NSA), with White House approval, engaged in wholesale surveillance of U.S. citizens, violating the Constitution in the process[49][50]. Much remains unknown about the extent of the operations, and both cases continue to unfold in the public media and the courts.

In December 2005, the *New York Times* published an article which revealed that "months after the Sept. 11 attacks, President Bush secretly authorized the National Security Agency to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required for domestic spying."[49] The program is unusual and troubling in a number of ways. To begin with, domestic intelligence gathering is normally the purview of the FBI, and the program represented "major shift in American intelligence-gathering practices, particularly for the National Security Agency, whose mission is to spy on communications abroad."[*ibid*] Also troubling was the apparent desire by the White House to keep the activities secret, not only from the public at large, but also from Congress and other government agencies. Although the program evidently began in 2002, it was not until 2004 that "for the first time, the Justice Department audited the N.S.A. program."[*ibid*]

Authorization for the domestic spying activities evidently originated directly from the White House. "Under a presidential order signed in 2002, the intelligence agency has monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of

people inside the United States without warrants."[49] No new laws to legally support the program were sought, because the Bush Administration "believed that the Congressional resolution on the campaign against terrorism provided ample authorization."[*ibid*] Key to the White House legal theory is the longstanding principle of expanded Presidential powers during wartime. Because of the state of conflict, "the government may be justified in taking measures which in less troubled conditions could be seen as infringements of individual liberties."[*ibid*]

It is important to note that a mechanism for legally performing domestic intelligence surveillance already existed, but that the Administration chose not to use it. The Foreign Intelligence Surveillance Court (FISA) is a special, secret court which oversees national security issues. "By getting warrants through the foreign intelligence court, the N.S.A. and F.B.I. could eavesdrop on people inside the United States who might be tied to terrorist groups without skirting longstanding rules."[49] Additionally, getting a warrant from the FISA court is easier than being granted one from a criminal court, as "the standard of proof required to obtain a warrant from the Foreign Intelligence Surveillance Court is generally considered lower than that required for a criminal warrant – intelligence officials only have to show probable cause that someone may be 'an agent of a foreign power'"[*ibid*].

The lengths which the government went to keep the eavesdropping program secret create suspicion that the NSA was involved in a more wide ranging operation than it appeared. In fact, it was the publication of the *Times* article that led Mark Klein, a former network engineer for AT&T, to disclose the evidence he had gathered which suggested that the NSA was not merely listening to domestic phone calls, but sifting through virtually all Internet traffic passing through the United States[50].

Klein worked at the site of a large SBC telecommunications facility at 611 Folsom St in San Fransisco, of which AT&T occupied three floors. "High speed fiber optic circuits come in on the 8th floor and run down to the 7th floor where they connect to routers for AT&T's WorldNet service, part of the latter's vital 'Common Backbone.'"[50] The routers at this facility served not only AT&T's network, but this location operated several "peering links" which connected AT&T and numerous other telecommunications providers, such as "QWEST... Global Crossing... UUNET, Level 3, Sprint... and Mae West. By the way, Mae West is one of two key Internet nodal points in the United States."[*ibid*]

In addition to the routing equipment, AT&T had also installed a splitter on the Internet cabling which led "to the 'secret room' on the 6th floor to monitor the information going through the circuits."[50] A splitter is a device for taking signal, in this case coming through a fiber optic cable, and making a copy of it so that the same signal (data) can go to two places. At the AT&T facility on Folsom St, all of AT&T's Internet traffic was split, with a copy diverted to Room 641A, the "secret room" to which only a single, NSA-cleared management worker had access[*ibid*].

While the specific purpose of the equipment housed in Room 641A is classified, Klein published a list of network devices operating in the room. Most notable among them is a Narus STA 6400: "The [Narus] STA Platform consists of standalone traffic analyzers that collect network and customer usage information in real time directly from the message...These analyzers sit on the message pipe into the ISP [Internet Service Provider] cloud rather than tap into each router or ISP device."[50] In other words, it looks at Internet traffic and analyzes not only the "envelope information" (such as the protocol in use, the addresses of machines communicating, and the time and date of the message), but also inspects the message content. According to expert analysis, "the Narus system is well suited to process huge volumes of data, including user content, in real time. It is thus well suited to the capture and analysis of large volumes of data for purposes of surveillance."[46] In short, the device is an Internet wiretap machine, and all the Internet traffic carried by AT&T at this location in San Fransisco (and the traffic of the other networks which had peering links to it) was being analyzed by the NSA, which AT&T had permitted to set up shop in their own office space.

The San Fransisco office was also not unique. Other documentation referred to the intelligence project as "Study Group 3", implying several other locations as well. "Seattle, San Jose, Los Angeles and San Diego are some of the rumored locations."[50] Analysis suggests that "it is highly likely that... [there exists] a fiber-optic network connected to the SG3 Secure Room, but separate and distinct from the [common backbone]. In other words, while the SG3 Secure Room is connected to the [common backbone]... it is also connected to another network, and signals can be sent out of or into the SG3 Secure Room"[46] through this network. With network surveillance facilities like the one on Folsom St scattered throughout the country, connected to large Internet connection points and coordinated through a separate private network with "Centralized Processing Facilities"[*ibid*], the NSA was in a position to spy on the entire Internet, with a system that "appears to have the ability to enable surveillance and analysis of Internet content on a massive scale, including both overseas and domestic traffic."[*ibid*]

RFID

Like most new technologies, Radio Frequency Identification (RFID) can be used in a wide variety of applications[51]. RFID systems, it seems however, have a unique ability to simultaneously excite and worry technologists everywhere. The question is not whether or not this technology will be used – it is already in wide deployment, and will soon be ubiquitous. Large retailers use it to track their shipments with fine-grained detail, and the technology is appearing in passports, identity cards, and mass transit systems.[*ibid*][52][53][54] The question which remains to be answered is how it will be used, and how it will be managed.

A basic RFID system consists of a *reader* and a *tag*. The reader, which can be about as small as

a juice box, is a device which broadcasts a specific radio signal to the surroundings. The tag, which contains a small chip and antenna in a package as small as a grain of rice, "listens" for the signal from the reader and replies with its own signal. Some tags contain only their unique identifier, similar to a bar code, whereas others can also store small amounts of additional data. Most importantly, while some tags may have some sort of power source (so-called "active tags"), many tags ("passive tags") can operate using only the power of the signal from the reader[55].

Their minuscule size combined with the ability for passive tags to function without power is why RFID presents a potential threat to privacy. The tag can be (and frequently is already) carried by someone who is completely unaware of its existence. Even if its presence is known, there is no way for the person carrying the tag to know when it is being queried, and blocking a tag requires isolating with a conductive material, such as a metal[56]. At its most benign, RFID can be used by commercial interests to track and data mine consumers more intensively, leading to more tailored and ubiquitous advertising. At the most extreme, RFID can be used by governments (or any powerful institution) to track every person at all times.

Conclusion

Surveillance is inextricably linked to modes of control. As such, any society not living under Lockean "natural law" will inevitably be subject to some degree of institutionalized surveillance. In fact, most surveillance technologies are created to serve a legitimate societal need, and generally serve the public good when balanced against other needs, such as individual freedoms and privacy. However, like all technologies, surveillance systems are subject to "function creep," and can gradually expanding in scope until they threaten to overthrow this balance. In such cases, a course correction is necessary to check the trend of increasing control, otherwise a free and open society may gradually transform into something else entirely. The interplay between technology and society is not static, and the responsible application of any technology depends on the constant reevaluation of its effects.

The history of surveillance mirrors the shifting needs of society as a whole. Radical technological developments almost always bring with them changes and challenges to the people who use them. The problems presented by the "technology" of slavery laid the foundations for the ID cards most of us use today. Likewise, the development of photography and biometrics during the last century have continued to influence our lives through the current technologies such as CCTV. However, more than any other development, the rise of computing machines has revolutionized our collective culture and permeates virtually every aspect of our lives.

The promise and the power of computers foreshadow the potential threat they pose. Like statistical analysis, computer technology is ethically neutral, but its application is not necessarily. Just as computers make it easier, cheaper, and faster to communicate with one another, they also have the

same effects for those wishing to listen to our conversations. An RFID-enabled ID card can reduce the time and hassle of airport security, but also reduce the time and hassle of following one's movements. A computer will serve any master, and whether they help or hinder us depends on how they are used, and by whom; the solution to the privacy problems introduced by surveillance are to be found with people, not technology. It is the careful design and application of policy which will ultimately maintain the balance between surveillance and privacy.

4. Present and Future Trends

The Value of Information

Information is power. But it is what you do with it that either makes you great or diminishes you.

Anonymous

The pursuit of power is an activity present throughout human history, one which seems unlikely end any time in the near future, if ever. Whereas some individual or group has always sought to exert power over another, the sources of that power change frequently. Power may be gained through possession of property, political sway, military might, industrial capability, control of critical resources, or any number of others. The introduction of computers and the development of information processing industry has increased the value of another resource: information.

The idea that information is power is not new. In virtually all fields, information can confer an advantage. For military commanders, intelligence about the enemy's position, strength, and tactics can decide the outcome of battles. Likewise, manufacturers continually seek knowledge of advanced techniques to improve their processes. In most cases, the power of information was derived from the specific application. The explosion of information production in recent years has introduced a relatively novel concept: the information economy. Now, as a tradable commodity, information can have value even if it lacks direct application. Strictly speaking, this has always been true, but the speed and ease with which information can be traded ensures that an interested buyer can always be found.

What has followed is an environment where information of all kinds, but especially personal information, is collected, aggregated, and sold repeatedly. Databases containing names, addresses, telephone numbers, and even sensitive data such as Social Security numbers are traded with whomever will pay the most. If oil was the prime trading commodity of the last hundred years, then information has replaced it for the coming century. Data is the coin of this new economy.

Present Trends

He who neglects the present moment throws away all he has.

Schiller

Current trends in the development and application of surveillance technology, placed in context through an informed understanding of its history, can help illustrate the overall condition of security

and privacy. By observing the current challenges and policies, we can understand not only where we presently stand, but can also begin to anticipate what the future holds. It is therefore extremely valuable to take stock of present movements in the sphere of privacy and surveillance.

The effect of recent shifts in the global security climate are still unfolding, but already significant consequences can be felt. The world, particularly the West, is overshadowed by a cloud of fear of global terror, and even minor risks and threats are treated with deadly seriousness. The natural response to risk is to minimize and control it, and that is frequently accomplished by gathering information. Thus, it is not at all surprising that surveillance currently has a powerful presence, and is leaving its mark on privacy.

Social Control

A common thread visible throughout the development of surveillance technologies is the need for prosecution or prevention of crime. Virtually every surveillance technology, from Bertillonage to wiretapping to CCTV, is "sold" to the public or justified *post hoc* on the merits of the technology's ability to ensure law and order. In fairness, many surveillance techniques do legitimately control crime: it would be difficult to argue against a list of convictions due to fingerprint evidence, to say nothing of the deterrent effect. Regardless, it is critical to evaluate the efficacy of surveillance systems and balance their costs in social and personal freedoms with their benefits in crime reduction. A system with only marginal impact on crime but significant impact on privacy fails to serve the public interest.

A prime example of the fallacious assumption of crime solving ability is found in the London CCTV example. If CCTV systems significantly aid in criminal convictions, then a strong correlation between cameras and crime solving should be apparent. The evidence, however, speaks differently: "A comparison of the number of cameras in each London borough with the proportion of crimes solved there found that police are no more likely to catch offenders in areas with hundreds of cameras than in those with hardly any."[57] While there are likely numerous explanations and compounding factors for this particular result, the key point is that these CCTV systems don't appear to be performing the task they are intended to. Nevertheless, new cameras are installed every year, despite evidence which suggests that better street lighting would have a greater impact on crime[*ibid*].

Fear of crime in general, and terrorism specifically, has dominated the public psyche in recent decades, and has risen markedly since September 11th, 2001. This climate of fear, combined with the danger of "function creep" inherent to surveillance systems, suggests that calls for increased surveillance should be viewed with a healthy skepticism. At best, the current trend of public fear and expanding government power is driving increasingly authoritarian and privacy-invasive policies, even in democracies. Worse, those calling for greater power for the state may harbor ulterior motives, and may stand to personally benefit from the power of harvested information. Although the current

situation is most likely the result of legitimate security concerns, the possibility of an ambitious individual or group subverting the state security apparatus for political gain is real. For evidence of this danger, one need look no further than the events of February 1933 in the short lived Weimar Republic.

At its most basic level, a surveillance system provides information, and by extension, power to its operator. At the national level, the surveillance operator is almost always the current government, therefore increased surveillance tends to give greater power to the incumbent political entity. When the form of government seeks to divide political power between competing groups, as is the case in the United States and most western democracies, a vast surveillance apparatus risks destabilizing the government by virtue of making one group more powerful than the others. Seen in this light, protection of individual privacy is not merely desirable, it is a prime safeguard against authoritarianism.

Marketing

Nowhere is the economic value of personal information more evident than in the world of commercial marketing. It is scarcely possible to complete a purchase without having one's name, address, telephone number, or at least ZIP code requested, even in "brick and mortar" stores, to say nothing of Internet businesses. When paying with cash, it is generally still possible to decline to give out such information, whereas paying with a credit card automatically releases some information. Even when releasing personal information is not mandatory, the frequency with which personal information is requested desensitizes people to the value of their information.

In certain industries, it has been found to be desirable to collect more detailed information about customers. Whereas the financial industry during the 1960's effectively forced customers to provide their Social Security number, businesses today mostly use an incentive approach. This practice usually takes the form of a "loyalty card" program, most commonly found in grocery stores, but also used in other retail outlets. In exchange for allowing the retailer to continuously monitor the customer's purchasing habits, a small discount or store credit is given. A similar system is used at toll booths, where customers who register themselves are given preferential treatment through dedicated lanes, enforced by RFID-enabled transponders.

On the Internet, where "free" is often the expected asking price for any service, the situation is carried to extremes. Most products and services available online are not truly free, but paid for with personal information. The ubiquitous registration process for everything from email accounts to video services ensures a continuous flow of information, all of which is aggregated, categorized, and sold repeatedly. One need only cast an eye over the tidal wave of unsolicited commercial email, or "spam," to see how quickly and widely personal information is disseminated.

As larger volumes of detailed personal information become available to commercial interests, increasingly detailed customer profiles emerge. Instead of merely discovering trends about their

customers as a group, retailers can discern the particular habits of individuals. The primary benefit of this fine-grained data for the retailer is targeted advertising. However, what also emerges is something that is best described as a "personality profile." Whereas advertising targeted at a particular customer's tastes is ideally more relevant and at worst merely annoying, information inferred from the detailed profile could have a significant impact.

Much of the commercial world's interest in understanding individual personalities can be traced to a marketing categorization system invented at Stanford Research Institute (SRI) during the 1970s. SRI found that "people could be defined by the different patterns of behavior through which they chose to express themselves. Self-expression was not infinite. It fell into identifiable types, and the SRI team invented a term for it: lifestyles."[58] Through analysis of survey results, consumers could be categorized by their "values and lifestyles," and their needs and desires predicted. Individualized purchase tracking takes this idea one step further: a customer's needs can be inferred from their choices, without the need to ask them directly through surveys. In this way, retailers can learn a great deal about the personal lives of their customers, including details they might not reveal if asked directly.

Information revealed through analysis of data like that collected by retailers has numerous applications beyond its original context. Once collected, it becomes the property of the owner of the database, and can be shared or sold to anyone willing to pay the asking price. Even prior to the TIA project, which had sought to combine government records with commercial databases in order to predict lawbreaking activity, data aggregation and analysis have offered to report specific, personal details for a price. One such firm boasts the ability to "determine whether you own a dog or a cat, enjoy camping or gourmet cooking, read the Bible or lots of other books. It can often pinpoint your occupations, the car you drive, your favorite vacations."[24, p. 107]

In many ways, how one acts reflects how one thinks. The greatest danger in allowing commercial third parties access to the intimate details of our lives is that it may give far too much insight into our personal thoughts. The local grocery store may only wish to sell a higher-margin product, but industry lobbies, political parties, and law enforcement could use the same information for considerably more potent purposes. Revealing too much personal information risks revealing thoughts which were intended to be kept private.

Social Networking

A relative newcomer to the information marketing world, "social networking" has already capitalized on the average Internet user's willingness to divulge all the details of their lives for a nominal benefit. Although the term can refer to a wide variety of services which feature interactions among their users, it is specifically socialization community sites like Facebook, MySpace, and their

countless facsimiles which are most interesting from a privacy standpoint. Not only is the collection of personal information a prerequisite for joining such a community, the entire *raison d'être* of such sites is the publication of this data.

One feature, in particular, of social networking sites is deserving of special attention. Virtually all communities provide a way for members to upload photographs which are then displayed with an optional caption, alongside their profile information. Although the user may have no qualms with publishing their own image online, other individuals featured in the photo may feel otherwise. The ability to caption photos enables association of so-called *metadata* which describes the contents, with the image. These features combine to form a mechanism where an individual can find their image, associated with their name, publicly posted on the Internet without ever being asked for permission. The person in question need not even be a member of the social networking community.

Google

The Internet search engine and advertising giant known as Google presents an unprecedented example of how computer technology and access to vast amounts of information can combine to form a potent threat to privacy, even with no ill intent. Despite the company motto of "Don't be evil,"[59] and their apparently earnest attempt to live up to his code, the company is by its very nature and market position a threat to privacy. With market share in the Internet search arena estimated at 63% and higher[60], Google is so dominant that its policies and products have instant, worldwide impact.

Each search query Google receives articulates what that user wishes to know at the moment: in effect, what they are thinking about. As search provider for the majority of Internet users, this puts the company in an enviable intelligence position. The U.S. Department of Justice already subpoenaed Google's search records in 2006, which to the search giant's credit, they resisted on privacy grounds[61]. As Google's knowledge of its users' activities grows, it becomes ever more attractive to law enforcement agencies worldwide.

Another way Google has raised hackles among privacy advocates is through the some of the new products and services they offer. For example, its GMail web-based email service has been criticized for its practice of using an automated advertising system which scans the contents of messages in an attempt to display relevant ads. Also controversial is the StreetView extension to Google's online map service, which provides street-level photographs of entire cities. Finally, it may only be a matter of time before Google is able identify individuals in photographs. The Image Search function has been able to recognize the presence of faces since 2007[62], and the ability to identify an individual from their face is a logical next step.

By all appearances, Google has gone out of its way to protect individual privacy and not abuse its market position. Good intentions, however, are often not enough, and the company will find itself

increasingly in the crosshairs of privacy activists as its power grows. Ultimately, the power Google has to know us and shape how we use information is emblematic not of their corporate ambitions, but of the power of information, and the general public's carelessness with its use.

Projected Developments

The future belongs to those who prepare for it today.

Malcolm X

Predicting the future is an inexact art, and if some of the predictions of the past are any indication, can be wildly inaccurate. Contrary to predictions, the automobiles of today are powered neither by rockets nor nuclear reactors, and sadly, cannot fly. On the other hand, the names of some science fiction authors are famous for their uncannily accurate depictions of future developments: authors such as Jules Verne, George Orwell, Isaac Asimov, and Arthur C. Clarke are celebrated for their prescient vision. Although never completely accurate, predictions can nevertheless help to visualize and prepare for the future.

Private

The effects of pervasive surveillance will first and foremost be felt in the private sphere. As every public action, movement, and transaction is recorded and analyzed, the contrast between private and public life will be amplified. The expectation of constant observation will lead to a state of constant self-policing and internalizing the gaze of the state[24, p. 180] whenever outside one's home. For some, particularly those born into these conditions, this will be unremarkable and possibly even comforting. Others, however, may find the constant stress of self-moderation too much, and may exhibit radical changes in personality, particularly when at home.

Compounding the effects of institutional surveillance, "personal surveillance" will increasingly be a factor. The phenomenon of "keeping up with the Jones'," already prevalent in American society, will reach new levels as friends and neighbors gain access to unprecedented levels of information about each other through social networking, personal weblogs, and home security systems. The constant fear of alienation resulting from a documented act of socially unacceptable behavior will create an environment of continuous vigilance, not only of the eyes of the state, but also of any associates.

Eventually, the resentment toward these invasions privacy will create a potentially violent anti-government and/or anti-corporate backlash. Small local revolutionary and paramilitary groups will spring up around the world. Capitalizing on the anonymity of the Internet, these groups will devise, evaluate, and share techniques for combating the surveillance system, such as methods of disabling

CCTV cameras or evading data mining analysis. Much like a low-level guerrilla conflict, sporadic bombings and other disruptions will result as the resisters gradually gain strength and confidence. These techniques and attitudes are already evidenced in modern anarchist movement, where anonymous message board posters brag about and celebrate acts of vandalism and sabotage against corporate interests, such as banks and conglomerates.

Commercial

The effects of surveillance and the ocean of data it makes available will be very different for the commercial world. The greater knowledge of customer desires and tastes will initially create new marketing paradigm, just as the inventions of the focus group and "values and lifestyles" system did in decades past. Coupled with detailed knowledge of the customer's tendencies and habits, widespread use of location-aware services which provide fine-grained tracking of customer's movements will allow commercial interests to build highly accurate models of each individual's life. For example, as an office worker is driving home from work, the entertainment system in his car will notice that it is Friday, and that grocery store records indicate he usually drinks beer on Friday evenings. In response, the system will helpfully suggest the latest seasonal brew from a national beverage concern and make a coupon available. Naturally, such valuable information will be shared with other retailers who are willing to pay for it.

However, as more private information becomes public, some data collection and mining operations will discover it to be more profitable if they limit access to their commodity. Companies who earn a reputation for higher quality analysis, or those with access to a greater amount of raw data will be able to charge a significant premium, ensuring that only the most powerful corporations can afford the most accurate analysis. Alternatively, the subjects of the data, the customers themselves, might be willing to pay a monthly fee in return for the suppression of their data. Commercial interests will fight among themselves for "information supremacy," and information monopolists will in a position to exert considerable influence over the marketplace and politics.

Ultimately, consumers will push back against overly-aggressive marketing, probably in response to a precedent-setting court case resulting in damages of millions. Eager to avoid government regulation, marketing companies will strike a compromise, dropping the most invasive practices in exchange for a "customer bill of rights." Such a document, drawn up either by government or a marketing trade association, would set limits on the use of personal data in exchange for a measure of certainty of what advertisers can be liable for.

Political

In the political sphere, the impact of new surveillance systems will vary widely. In countries

where the stability of the group is typically held in higher regard than individual freedoms, such as China, the state may acquire some new tools, but for the most part it will be business as usual. In contrast, regions with a strong tradition of individuality, like most Western democracies, will encounter political turmoil. The degree to which surveillance technology is applied and the government response to popular resistance will determine how great the upheaval will be.

Social-democratic nations like Germany and France will, after an initial experiment with more aggressive surveillance, scale back their operations and work to regulate the flow and use of information in both the private and public sector. The United Kingdom, which is already today the leader in invasive, routine surveillance, will likely not relent, and experience a gradually accelerating shift towards authoritarianism in response to popular resistance. The United States, currently dominated by fears of terrorism and in the midst of expanding its surveillance machine, risks following the British model. However, with the passage of time and increasing emotional distance to the events of 9/11, the strong libertarian streak in American culture will reassert itself and reign in government control.

Further effects of a ubiquitous surveillance regime will be evident in socio-political classes. Differing levels of education will elicit vastly different reactions to the expanding power of industry and government. Among the educated elite, concerns about the loss of freedoms will foster discussion and effective organization. Those with the resources to do so will avail themselves of social and legal tools to protect themselves. The less educated, particularly the uneducated poor, will find themselves unable to effectively resist. Moreover, short term financial incentives will convince many to "opt in" to systems which do not benefit them in the long term. The resultant dissonance between the classes will reinforce already present divisions, and increased social unrest is to be expected.

Conclusion

No technology exists in a vacuum, and every social and technological development has an impact which extends far beyond its immediate area of concern. Every invention carries with it unintended consequences, and to believe that the expansion of surveillance technology will result only in more effective advertising and safer streets is dangerously shortsighted and naïve. While the details of these predictions may prove to be incorrect, it is absolutely imperative we keep an eye to the future. Failure to anticipate future developments will leave us with only the repression and suffering we already encountered in the past.

5. Recommendations and Conclusion

Introduction

As has been shown, there are many forms of surveillance technologies, and many ways that privacy can be violated. Surveillance is employed by governments, employers, advertisers, retailers, and everyone in between. In order to protect privacy, the response must be equally multifaceted. It is not enough to worry only about government spying, as the commercial sector could also have equally devastating effects. Likewise, blindly trusting governmental power is a surefire recipe for losing control of one's information and rights. There are many avenues which can be explored to protect individual privacy: some are techniques which can be exercised by individuals, and others require political action.

Public Policy

The government is arguably the party which exercises the most power over individuals. It has the power to protect us, tax us, conscript us, and incarcerate us. It is therefore natural that the government is in a position to exercise immense power over our privacy, both to our benefit and detriment. According to democratic principles, however, the power of government is not infinite. If it acts against the interests of the people it represents, then the people have the right and duty to change it.

Some of the ways in which the government invades our privacy are simply the costs for the safety and security we demand. Although we may not enjoy submitting to a police search, we understand that the ability for police to perform searches and arrests helps protect us from others who would violate our rights. Still, when the law enforcement and intelligence arms of our government overstep their bounds, we must force a change or else allow them to continually encroach on our rights. The recent revelations of wholesale, routine, and secret dragnet surveillance perpetrated by the U.S. government against its own people must not be allowed to go uncorrected. To do so would set a dangerous precedent, and propel us down a path we have already traveled too far.

Constitutional Amendment for Privacy

The lack of explicit privacy protections in the U.S. Constitution represents a major vulnerability to the American citizen. Although the Framers of the Constitution should not be faulted for this oversight – none of the modern surveillance technologies existed at the time – the lack of privacy protection should also not be viewed as a necessary feature of the document. Knowing full well that all future eventualities could not be foreseen, the Framers built into the document a mechanism for adding needed features later: the Constitutional Amendment. The U.S. Constitution has been amended

numerous times already, and for far more frivolous matters, such as the prohibition of alcohol. Protecting personal privacy is certainly important enough to warrant an Amendment.

The specific language and details of such an Amendment is up to Congress to decide, and far beyond the scope of this document. There is enough documented experience with privacy issues in U.S. legal history to provide a helpful guide to policymakers. Furthermore, it would be prudent to build upon the experience of others in this arena, and to model the change on similar documents, such as the European Directive on Data Protection. The legal history shows that the need for protecting individual privacy is a recurring theme, and advances in technology will only emphasize its importance. One of the most important steps the United States can take to ensure the rights of its citizens are not trampled is to formally recognize their importance in its highest laws.

Private Actions

Despite the array of technology employed against individuals to capture and exploit their personal information, much of the blame for the current state of privacy protection lies with those very individuals. In many ways, it is the complacency and lack of concern of one's personal information that has brought us to this point. Granted, decades ago there was little utility in knowing someone's name and address, unless you wished to knock on their door. Nevertheless, the situation has changed, and most people are at least vaguely aware of the possibilities. Ignorance may explain the cavalier attitude many people have towards protecting their own privacy, but it does nothing to mitigate the damage done when exploited.

Education of the general public about privacy matters is critical to the success of any attempt to empower individuals to protect themselves. Awareness of the value of personal information will make people take notice when this information is requested, and cause them to question the reasons. If enough people demand answers every time their government or retailer asks for their name or address, the collection of information will become less routine, and only requested when truly necessary.

Encryption Everywhere

The single most effective technique a private individual can employ to protect their privacy is the encryption of data whenever and wherever feasible. Specifically, it is public key encryption which has the potential to revolutionize Internet privacy. This method of obfuscating data, which is present in all modern web browsers and available in purpose-built encryption software such as Pretty Good Privacy (PGP), relies on the fundamental mathematical difficulty of certain calculations to secure data. Although the algorithm employed by these encryption schemes is not secret and is publicly available, the amount of time necessary to forcibly decrypt a message, even with vast computing resources, makes it completely impractical to do so. Put another way, all the governments in the world, using all

the computers available to them, would be unable to crack the code because it *simply takes too long*.

Email and instant messaging, two mediums through which many people share very sensitive information, generally have no security whatsoever built in: the message contents are plainly visible to anyone who can capture the data in transit. Voice-Over-IP (VOIP), essentially Internet telephone, is another sensitive case. Although some VOIP applications, such as Skype, do encrypt calls, the method of encryption may be secret and therefore of unknown reliability, as is the case with Skype. Virtually all forms of Internet data surveillance can be thwarted by the application of public key encryption, and because encryption acts as a "wrapper" for the message data, virtually any application can benefit.

Encryption is not a panacea for all surveillance problems, however. In order to be effective, the so-called "private key" which is to generate the encrypted message must be kept confidential. Additionally, vulnerabilities exist at the endpoints of the communication, before encryption and after decryption, which can also be targeted by motivated parties. Further safeguards, such has full-disk encryption, may be used to guard against these contingencies. It should be noted, though, that an entity with the resources of a government agency which has targeted a specific individual for spying will most likely get the information they seek. It is routine, dragnet surveillance which encryption guards against best, and as such represents a powerful first line of defense.

Conclusion

Protecting privacy is a complex issue. In a world where clandestine criminal operations can bring death and destruction to thousands in the blink of an eye, it is easy to mistake personal privacy as somehow optional: nice to have, but trumped by other, more pressing concerns. Nothing could be further from the truth. Privacy is the foundation upon which all of our rights as citizens rest. Take away our privacy, and we stand naked before the power of our government, supremely vulnerable to its whims. We must never forget that it is government which should be subject to our whims, and not the reverse.

Despite the lack of explicit Constitutional protection for privacy, the United States has a long history of affirming and defending this right for its citizens. Well over a century of legal cases and a far longer social tradition demonstrate that the right to privacy is an important part of what it means to be an American. Still, the protections afforded by the government are incomplete and shifting. More must be done if the tradition of individual freedoms is to survive the current and future technological developments.

Like privacy, the technology and techniques of surveillance are also ingrained in our culture. Surveillance technologies are not developed to enslave the people, but to serve a specific and valuable need. However, like all technologies, they find uses outside of the scope in which they were conceived,

and must be continuously monitored and their application adjusted if they are to remain in the public service. Most importantly, when they cease to act in the public good, they must be retired.

Although there are many challenges to the protection of personal privacy, there are also a number of tools which are available to be called in its service. Chief among these are public awareness and personal empowerment. By actively monitoring and protecting our personal data, we can hold accountable those who wish to use it. Ultimately, no one can forcibly remove our right to privacy – but take it for granted, and we may not even notice that we've been giving it away.

References

[1] *Griswold v. Connecticut*, 381 U.S. 479, 1965
[2] Clarke, Roger, "What's Privacy?", August 2006. http://www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html
[3] Alderman, Ellen; Kennedy, Caroline, *The Right to Privacy*. New York: Alfred A. Knopf, Inc., 1995.
[4] *Boyd v. United States*, 116 U.S. 616, 625, 1885
[5] *Bell v. Wolfish*, 441 U.S. 520, 1979
[6] *Schmerber v. California*, 384 U.S. 757, 767, 1966
[7] *Terry v. Ohio*, 392 U.S. 1, 21-22, 1968
[8] *Gerstein v. Pugh*, 420 U.S. 103, 113, 1975
[9] *McCarthy v. Arndstein*, 266 U.S. 34, 1924
[10] *Malloy v. Hogan*, 378 U.S. 1, 1964
[11] *Chambers v. Florida*, 309 U.S. 227, 1940
[12] *Haynes v. Washington*, 373 U.S. 503, 1963
[13] *United States v. Sullivan*, 274 U.S. 259, 1927
[14] *Garner v. United States*, 424 U.S. 648, 1976
[15] *Hiibel v. Sixth Judicial District Court of Nevada*, 542 U.S. 177, 2004
[16] *Lochner v. New York*, 198 U.S. 45, 1905
[17] *Adkins v. Children's Hospital*, 261 U.S. 525, 1923
[18] *West Coast Hotel Co. v. Parrish*, 300 U.S. 379, 1937
[19] *Eisenstadt v. Baird*, 405 U.S. 438, 1972
[20] *The Privacy Act of 1974*, 5 U.S.C. 552a, 1974
[21] Statewatch, "EU-USA PNR: US changes the privacy rules to exemption access to personal data", September 2007. http://www.statewatch.org/news/2007/sep/04eu-usa-pnr-exemptions.htm
[22] United States Department of Health & Human Services, "Summary of the HIPAA Privacy Rule", May 2003
[23] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, H.R. 3162, 107th Congress (2001).
[24] Parenti, Christian, *The Soft Cage: Surveillance in America*. New York: Basic Books, 2003.
[25] Lichtblau, Eric, "Senate Approves Bill to Broaden Wiretap Powers," *New York Times* [Online], July 10, 2008. http://www.nytimes.com/2008/07/10/washington/10fisa.html
[26] American Civil Liberties Union, "Supreme Court Refuses to Review Warrantless Wiretapping Case", February 2008. http://www.aclu.org/safefree/nsaspying/34152prs20080219.html
[27] Council of Europe, "Convention for the Protection of Human Rights and Fundamental Freedoms", November 1950. http://conventions.coe.int/treaty/en/Treaties/Html/005.htm
[28] Organization for Economic Cooperation and Development, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", September 1980. http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html
[29] European Parliament, Council, "Directive 95/46/EC on the protection of personal data," *Official Journal of the European Communities*, No. L. 281, p. 31, 23 November 1995
[30] *Identifying Numbers*, 26 U.S.C. 6109, 1961
[31] GAO-04-548, *Data Mining: Federal Efforts Cover a Wide Range of Uses*, United States General Accounting Office, May 2004.
[32] William Seltzer, "The Promise and Pitfalls of Data Mining: Ethical Issues," 2005.
[33] Lyman, Peter; Hal R. Varian, "How Much Information," University of California at Berkeley, 2003.
[34] Fayyad, Usama; Piatetsky-Shapiro, Gregory; Smyth, Padhraic, "From Data Mining to Knowledge

Discovery in Databases," 1996.
[35] National Association of State Chief Information Officers, "Think Before You Dig: Privacy Implications of Data Mining & Aggregation," 2004.
[36] "TRACES OF TERROR; Excerpts From Senate Judiciary Committee's Counterterrorism Hearing," *New York Times* [Online], June 7, 2002. http://query.nytimes.com/gst/fullpage.html?res=9506E7D8143DF934A35755C0A9649C8B63
[37] Williams, Mark, "The Total Information Awareness Project Lives On: Technology behind the Pentagon's controversial data-mining project has been acquired by NSA, and is probably in use", *Technology Review,* April 2006. http://www.technologyreview.com/Infotech/16741/
[38] Hempel, Leon; Töpfer, "Working Paper No. 1: Inception Report," Centre for Technology and Society, Technical University Berlin, January 2002.
[39] McCahill, Michael; Norris, Clive, "Working Paper No. 6: CCTV in London," Centre for Criminology and Criminal Justice, University of Hull, June 2002.
[40] "Big Brother is shouting at you," *Daily Mail* [Online], September, 2006. http://www.dailymail.co.uk/news/article-405477/Big-Brother-shouting-you.html
[41] Simpson, Gemma, "'Big Brother' cameras listen for fights," *CNET News* [Online], November 22, 2006. http://news.cnet.com/Big-Brother-cameras-listen-for-fights/2100-1029_3-6137888.html
[42] "CCTV network tracks 'getaway car'," *BBC News* [Online], November 21, 2005. http://news.bbc.co.uk/2/hi/uk_news/england/bradford/4455918.stm
[43] Tanneeru, Manav, "'Ring of Steel' coming to New York," *CNN* [Online], August 3, 2007. http://www.cnn.com/2007/TECH/08/01/nyc.surveillance/index.html
[44] PC Magazine, "wiretapping Definition", February 2009. http://www.pcmag.com/encyclopedia_term/0,2542,t=wiretapping&i=54791,00.asp
[45] *Katz v. United States*, 389 U.S. 347, 1967
[46] Marcus, J. Scott, "Declaration of J. Scott Marcus in Support of Plaintiffs' Motion for Preliminary Injunction," *Hepting v. AT&T*, C-06-0672-VRW, Northern District Court of California, June 8, 2006.
[47] Communications Assistance for Law Enforcement Act, H.R. 4922, 103rd Congress (1994).
[48] Electronic Communcations Privacy Act of 1986, H.R. 4952, 99th Congress (1986).
[49] Risen, James; Lichtblau, Eric, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times* [Online], December 16, 2005. http://www.nytimes.com/2005/12/16/politics/16program.html
[50] Klein, Mark, "AT&T's Implementation of NSA Spying on American Citizens," *Wired Magazine* [Online], December 31, 2005. http://blog.wired.com/27bstroke6/att_klein_wired.pdf
[51] RFID Journal, "Frequently Asked Questions: What are some of the most common applications for RFID?", February 2009. http://www.rfidjournal.com/faq/16/56
[52] Nakashima, Ellen, "Electronic Passports Raise Privacy Issues," *Washington Post* [Online], January 1, 2008. http://www.washingtonpost.com/wp-dyn/content/article/2007/12/31/AR2007123101922.html
[53] Associated Press, "New York to offer enhanced driver's license," *Newsday* [Online], September 16, 2008. http://www.newsday.com/services/newspaper/printedition/tuesday/news/ny-nylice165845220sep16,0,5665783,print.story
[54] Broersma, Matthew, "Smart-card ticketing goes Underground," *ZDNet* [Online], November 20, 2002. http://news.zdnet.co.uk/hardware/0,1000000091,2126235,00.htm
[55] Sheridan, Valery; Tsegaye, Binyam; Walter-Echols, Michael, "ZigBee-Enabled RFID Reader Network," Worcester Polytechnic Institute, March 4, 2005.
[56] Baard, Mark, "Is RFID Technology Easy to Foil?," *Wired* [Online], November 18, 2003. http://www.wired.com/politics/security/news/2003/11/61264
[57] Davenport, Justin, "Tens of thousands of CCTV cameras, yet 80% of crime unsolved," *Evening Standard* [Online], September 19, 2007. http://www.thisislondon.co.uk/news/article-23412867-

details/Tens+of+thousands+of+CCTV+cameras%2C+yet+80+of+crime+unsolved/article.do
[58] Curtis, Adam, *The Century of the Self*, "Part 3: There is a Policeman Inside All Our Heads: He Must Be Destroyed", *BBC* [Documentary], 2002
[59] Google, Inc., "Google Code of Conduct", February 1 2008. http://investor.google.com/conduct.html
[60] Stross, Randall, "Everyone Loves Google, Until It's Too Big," *New York Times* [Online], February 21, 2009. http://www.nytimes.com/2009/02/22/business/22digi.html
[61] Penenberg, Adam L., "Google vs. DoJ," *Slate* [Online], January 25, 2006. http://www.slate.com/id/2134767/
[62] Cheng, Jacqui, "Facial recognition slipped into Google image search," *Ars Technica* [Online], May 30, 2007. http://arstechnica.com/old/content/2007/05/facial-recognition-slipped-into-google-image-search.ars