Sensors in Public Spaces:

The Law and Technology of Anonymity

Co-authors
Shuvo Chatterjee
Mabel Feng
Brian Keegan
Sarah Ma
Jennifer Wang

December 10, 2004

6.805/STS.085

Acknowledgements

We would like to thank the staff of 6.805, “Ethics and Law on the Electronic Frontier.” They have helped us immensely in providing critiques, feedback, topic ideas, and more. In particular, we thank Michael Fischer for really helping us to shape our research. Hal Abelson for his suggestions on case studies. Keith Winstein for coming up with scenarios that stumped us and challenged us to reshape our recommendations and PAPA.

Other people we would like to thank who assisted us throughout our research include: Professor Granger Morgan, Engineering and Public Policy, Carnegie Mellon University; Elaine Newton, Engineering and Public Policy, Carnegie Mellon University; Dalie Jimenez, aide to Massachusetts State Senator Jarrett Barrios; Pamela Kogut, Massachusetts Assistant Attorney General for Consumer Protection; and Chief John DiFava, chief of police, Massachusetts Institute of Technology.

Table of Contents

Executive Summary

Increasingly, public spaces are filling with non-obvious and interconnected monitoring technologies whose data collection, storage, processing, and distribution capabilities have to potential to invade one's expectation of anonymity. We examined four groups of technologies – surveillance cameras, the Internet, radio frequency identification (RFID) tags, and biometrics – and developed anonymity policy recommendations under a comprehensive Public Anonymity Protection Act (PAPA). In order to develop these policies and legislative proposals, we examined basic Constitutional principles interpreted though key judicial cases, current legislative statues, and the challenges presented by these four sensing technologies towards implementing the policy. We evaluated these challenges by employing a framework that compares the invasiveness of a sensor given its human functional equivalent, potential for opting-in, pervasiveness, and its location on the identification potential spectrum. The identification potential spectrum assesses a sensor's ability to identify individuals by the extent to which data is collected, stored, processed, and distributed. Passive technologies have the capability of implicitly identifying or locating an individual because they collect and store data. Active technologies explicitly identify or locate an individual because of their ability to process and distribute data. The potential for sensors to invade a reasonable expectation of anonymity in public spaces is greater for active technologies that collect large amounts of data, store data for unnecessarily long times, process, analyze and distribute data.

Problem Statement

Imagine walking in a park or down a busy street. Someone you do not know approaches you. With no introduction or pretext, she asks you, ”What is your address and telephone number?” Certainly this would be unexpected and unsettling. You may think to yourself, “Who is she? Why does she want this information? What is she going to do with this information? What kind of nerve does she have to ask me this?” Of course you don't tell her. There is no law or statue that would require you to disclose any information about yourself to another person. However, this thought never crosses your mind because you are more focused on now avoiding this person who has tried to invade your privacy.

Now imagine a man you have never met before approaches you and addresses you by your Social Security Number. You may or may not have realized he was following you. After your previous encounter you are already unsettled, but now having had two people you've never met trying to obtain your personal information, you are shaken.

As you attempt to enter a bar to escape these two unexpected encounters, the bouncer stops you and asks you for identification. As you present your driver's license, he dials his cell phone and begins reading your name, driver identification number, and organ donor status to his buddy on the other end. Outraged, you grab your ID and turn around. You can tell the stalking man had overheard the call and was already telling the curious woman. Since when did being in a public place mean having to surrender your

anonymity?

Now imagine all day different people tried to interrogate you for personal information and follow you around wherever you went. This happens everyday, but it does not involve random people. It happens without your seeing, knowing, or consenting to having your privacy invaded. It involves sensors in public spaces capable of generating and sharing data about every aspect of your life. What may have previously constituted an invasion of privacy when perpetrated by a human is now commonly done with technology. Video cameras, electronic networks, radio identifiers, biometrics, and a plethora of other technologies interrogate us daily for personal information and we willingly oblige. While we accept these technologies because they are efficient and often integrated into our routines, their ability to store, analyze, and distribute data can increasingly track our movements and identify us even when we wish to remain anonymous.

Definitions

Sensors systems generate data based upon the environment with which they interface. The sensor system generates data using collectors, storage, processor, and a distributor.

A public space is defined as a space that meets at least one of the following characteristics: provided for and used by the government, accessible, visible to the public, shared by all members of a community and an area in which individuals may engage in public behavior.

Privacy is understood to be the ability to control the disclosure of personal information, bar intrusion into personal space, guard against the misuse of personal information, protect one's identity as a form of property, or the "right to be left alone."[1]

Anonymity is a subset of privacy wherein an individual has the right to conduct transactions and otherwise interact with others without identifying himself.

Identification is the absence of anonymity, when one's personal information is no longer private.

Personal information is unique and identifiable data. It could be one's name, date of birth, race, ethnicity, age, religion, social security number, telephone number, network address, license plate, health status, marital status, financial status, sexual orientation, arrest record, group membership, political affiliation, fingerprint, voice signature, optical pattern, or any other unique, identifiable, and non-anonymous data.

[1] Legal Information Institute. Cornell Univeristy. *Law about... right of privacy*. http://www.law.cornell.edu/topics/privacy.html

Analysis Framework

This is the analysis framework we used to evaluate privacy and anonymity concerns in this paper.

Human-Functional Equivalent

Sensors, unlike humans, are not limited in the data they may collect. The human functional equivalent describes analogous human actions to a sensor's function. By stripping away the technical features and anthropomorphizing sensors based upon the functions they perform, their capability and use can be more appropriately framed for legal analysis. The human functional equivalent of a video surveillance camera would be a police officer standing on a street corner. He may be collecting and temporarily storing data, but his ability to process and distribute this data is constrained by human limitations. The range of human actions and public nuisances legally defined to be invasive, noisome, dangerous cannot be directly applied to sensor technologies. While either humans or sensors may invade on an individual's privacy, both should be held to similar standards of protecting his expectation of privacy in public spaces. Because the technological sensors exceed the human capabilities of to invade privacy and anonymity, they are a more ideal target for legislation.

Consent

Opt-in or opt-out schemes grant individuals choice to participate in a system. For sensors, this might entail choosing not to use collectable or identifiable entities, like ID cards. It may also be choosing not to allow one's data to be stored, processed, or distributed after collection. If a sensor cannot provide such a choice, it may lend to more readily infringing upon one's right to privacy and should then be regulated.

Pervasiveness

The pervasiveness of sensor systems determines to great effect how accepted or ingrained it becomes. Certainly the limited capability of human senses to see and hear and invade privacy are extremely pervasive and could not be enforceable or regulated. However, developing technologies incorporating features with a far greater potential to invade one's privacy are not yet commonplace. Those sensors that are not commonplace may be subject to different rules than those that have become pervasive.

Identification Potential Spectrum

Sensors share common features: the collection, storage, processing, and distribution of data. Any one of these features is not enough warrant serious concerns about privacy. We develop a spectrum model delineating the potential for sensors to passively or actively identify individuals. A spectrum is a distribution of characteristics rather than a discrete state and ours ranges from passive features to active features. An active sensor does not necessarily invade one's privacy, but rather has a greater potential to do so than a more passive technology.

Collection is process of capturing and inputting data into the system. Every piece of information that

enters a system does not necessarily become data. This selectivity is an important distinction. Some data can be abstracted and can only selectively interact with specific sensors, as in a bar-code and laser system. But it is also possible to collect less specific information like light and electromagnetic waves. The data collected is not necessarily identifiable at this point.

Storage is the retention of data within the system. The data entering the system is of little value if the sensor collects more data at a later time and overwrites or erases the previous data. Magnetic media like tapes and hard drives, electronic media like flash or random-access memory, or other storage media retain make data available at a later time.

Processing creates new data from stored data. By combining, analyzing, or mining data, computations can create connections between different data and reveal patterns or trends. This is the step where identification occurs.

Distribution is the output of data from the sensor system. Data can be physically distributed on storage media or electronically distributed over networks. Distributed data can be used for separate storage or processing applications or to provide inputs to other systems. The ability to transmit data raises the problem of security and permitting only authorized parties to receive sensor data.

Because different technologies exhibit different features, they occupy different locations on the spectrum relative to their potential to infringe on privacy and anonymity. Passive sensors feature collection and limited storage but can only implicitly identify an individual by analysis outside of the sensor system. Active sensors have a greater potential to explicitly identify individuals because their design incorporates processing and distribution features within the sensor system. Sensors incorporating more active features like processing and distribution are may invade one's privacy by the nature of their efficiency in processing and distributing data. Sensors using passive features like collection and storage are less capable but nevertheless equally liable to invade an expectation of privacy by collecting non-specific data and storing it indefinitely.

Law and Values

The notion of anonymity as a kind of privacy is tied with the ability to control information about oneself. What is developed below is an argument that there exists a personal sphere even and an expectation of anonymity that may be invaded or intruded upon even in public spaces. An individual has a right to expect privacy in these zones because such a right is guaranteed by implication from other explicit rights.

Privacy has been defined as a freedom from unauthorized intrusion, to be let alone, right of a person to be free from intrusion into or publicity concerning matters of a personal nature.[2] The courts have

[2]Legal Information Institute. Cornell University. *Law about... right of privacy: personal autonomy.*

recognized privacy in different ways: an expectation of privacy, an invasion of privacy, a right of privacy, and a zone of privacy.

An expectation of privacy **is** a belief in the existence of freedom from unwanted or governmental intrusion in some thing or place. The law recognizes the private nature of conversations between lawyers and clients, doctors and patients, and spouses as confidential.[3] These information conveyed by parties in these conversations have the expectation of privacy because they contain personal information.

An invasion of privacy **is** a tort of unjustifiably intruding upon another's right to privacy by appropriating his or her name or likeness, by unreasonably interfering with his or her seclusion, by publicizing information about his or her private affairs that a reasonable person would find objectionable and in which there is no legitimate public interest, or by publicizing information that unreasonably places him or her in a false light.[4]

A zone of privacy **is** an area or aspect of life that is held to be protected from intrusion by a specific constitutional guarantee or is the object of an expectation of privacy. The Fourth Amendment establishes the right to be secure in one's person, house, papers, or effects against unreasonable searches or seizures. One's person, house, papers, and effects are then a zone of privacy.

A public space is not consistent with the notion of privacy because public spaces are not private. The Constitution explicitly protects one's private residence from intrusions by the state in the Fourth Amendment. The principle of an expectation of privacy is altered in a public forum where a space is known, accessible, visible, and shared by the general population. Because the state of being in a public space is non-secluded and non-private, there are intrusions upon one's privacy that are not protected.

Nevertheless, simply being in a public space does not compel one to make his identity known. Herein lies the difference between privacy and anonymity. Anonymity is the right to conduct one's actions publicly: to be able to live, work, and contribute to the public sphere, without needing to identify oneself. This notion of anonymity is tied to the personal liberty and freedoms protected in the Constitution. The Constitution is not a list of freedoms, but of rights retained by individuals to check the power of government. Many freedoms are not explicitly stated, but are instead understood to be extended from these specific rights. The courts have developed a notion of a penumbra, or a body of rights, held to be guaranteed by implication from other rights explicitly enumerated in the U.S. Constitution.

---

http://www.law.cornell.edu/topics/personal_autonomy.html.

[3] Law.com Law Dictionary..*Priviliged communication*. http://dictionary.law.com/default2.asp?selected=1615&bold.

[4] FindLaw Constitutional Law Center. *Invasion of Privacy*. http://supreme.lp.findlaw.com/constitution/amendment01/19.html.

Griswold v. Connecticut

Griswold v. Connecticut develops the notion that there are kinds of privacy, while not explicitly stated, that are nevertheless protected by the Constitution. A physician and executive associated with Planned Parenthood of Connecticut were convicted as accessories for providing married persons information, medical advice, and prescriptions for contraceptive devices in violation of Connecticut statues criminalizing the use of contraceptives. The appellants claimed this statue violated the Fourteenth Amendment and deprived them of equal protection of laws.[5]

The Supreme Court in 1965 affirmed this judgment as an unreasonable infringement on marital privacy.

> Such a law cannot stand in light of the familiar principle, so often applied by this Court, that a governmental purpose to control or prevent activities constitutionally subject to state regulation may not be achieved by means which sweep unnecessarily broadly and thereby invade the area of protected freedoms.[6]

However the majority opinion develops an interesting framework of implicit rights derived from the explicit Constitutional rights. The notion of marital privacy falls within "the penumbra of specific guarantees of the Bill of Rights." This progressive interpretation of the Constitutional encompasses rights that while they are:

> not mentioned explicitly in the Constitution, are supported both by numerous decisions of this Court, referred to in the Court's opinion, and by the language and history of the Ninth Amendment. ...[The Ninth Amendment] was proffered to quiet expressed fears that a bill of specifically enumerated rights could not be sufficiently broad to cover all essential rights, and that the specific mention of certain rights would be interpreted as a denial that others were protected.[7]

The Ninth Amendment protects those rights that are neither explicitly stated nor listed in the Constitution. The justices held that this ability to interpret the Constitution strengthens the explicit rights because they are not limited or constrained. In Griswold, the Court derived such peripheral rights, like marital privacy, are constitutionally protected though no such right is explicitly stated.

> "Without those peripheral rights, the specific rights would be less secure. Various [Constitutional] guarantees create zones of privacy."[8]

These conclusions are significant because the Court recognizes that there are rights implicitly protected by the Constitution. Moreover, this case highlights a case where government attempts to monitor and control the actions of private citizens were found to be excessively invasive despite arguments attesting to the public utility of such invasions to enforce a prohibition. There exists a right for citizens to be free from government monitoring.

---

[5] *Griswold v. Connecticut*. 381 U.S. 479, Syllabus. (1965).
[6] *Griswold v. Connecticut*, Opinion of the Court.
[7] ibid
[8] ibid

Katz v. United States

Katz v. United States is a repudiation of an earlier ruling (*Olmstead v. United States*) and establishes that the Constitution protects protect “people, not places” from government searches. Katz was convicted of transmitting wagering information over state lines by using a public telephone booth to avoid wiretapping. FBI obtained evidence by attaching an electronic listening and recording device to the exterior of the booth. The question facing the court centered on Fourth Amendment protections in a public space. The Court of Appeals affirmed the conviction claiming Fourth Amendment protects physical locations and the present case involved "no physical entrance into the area occupied by" Katz.[9]

The Supreme Court reversed this decision in 1967. It recognized Katz's calls in the phone booth as constitutionally protected activities. Furthermore, this case demonstrates the evolution of the understanding between law and technology. Eavesdropping activities constituted a “search and seizure” from which the Fourth Amendment protects oral statements as well as tangible items (persons, houses, papers, and effects). The Court also reversed the “trespass” doctrine of an earlier case (Olmstead v. United States) involving evidence gained from wiretapping a telephone. The court emphasized the Fourth Amendment “protects people, not places.”[10]

> These considerations do not vanish when the search in question is transferred from the setting of a home, an office, or a hotel room to that of a telephone booth. Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.[11]

By doing so, it established a new paradigm for evaluating the balance between search and privacy. There exists a zone of privacy even in public areas upon which one may justifiably rely upon and for which there may be an unreasonable intrusion or invasion.

> What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[12]

In a concurring opinion, Justice Harlan attempted to identify what rights are granted to the people and the activities that occur in these places. In what would become the “Katz test”,

> First that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable."[13]

The court, in deciding the protections granted by the Fourth Amendment to searches and seizures in public places, did not go so far as to extract this amendment as a general right of privacy.

> But the protection of a person's *general* right to privacy -- his right to be let alone by other people -- is, like the protection of his property and of his very life, left largely to the law of

---

[9] *Katz v. United States*. 389 US 347, Syllabus (1967).
[10] *Katz v. United States*, Opinion of the Court.
[11] ibid
[12] ibid
[13] *Katz v. United States*, Concurring Opinion.

the individual States. [14]

Katz was a landmark case for privacy rights because it began to crystallize the concept of privacy rights existing even within a public sphere. The Constitution protects more than the items and places cataloged in the Fourth Amendment (persons, houses, papers, and effects). This distinction is important because it guarantees individuals a margin of privacy – that "which he seeks to preserve as private" - in the public sphere that had not previously been recognized.

Kyllo v. United States

The Supreme Court in *Kyllo v. United States* established a balance between an individual's expectation of privacy and the ability for a sensor to determine the individual's actions. Kyllo was suspected of growing marijuana in his residence. Federal agents used a thermal imager to detect heat emanating from high intensity lamps used to grow marijuana indoors. Based in part upon this imaging, a judge issued a search warrant for the residence where marijuana was found. Kyllo moved to suppress this evidence on grounds that it was obtained from an illegal search.[15]

The Supreme Court in 2001 held the use of this technology to obtain information on the interior of a house as an unreasonable search. Like Katz, the Kyllo decision demonstrates that Constitutional protections do not disappear with the application of new technologies. However, in addressing the question or uncertainty of possible future technological capabilities, the Court determined the pervasiveness of technologies contributed towards its legality.

> Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a "search" and is presumptively unreasonable without a warrant. [16]

The Court recognized there exists a minimal expectation of reasonable privacy which is protected from erosion by technology that is not in general public use. Furthermore, the Court did not subject Fourth Amendment protections to mechanical or physical interpretations or tests. Though the information in the form of energy may have left the property much like the sound waves leaving the phone booth in *Katz*, the Fourth Amendment is not limited by trespass, but protects against intrusions on reasonable expectations of privacy by unreasonable searches.

Nader v. General Motors Corporation

Nader is a significant case because it recognizes that an individual does not lose every expectation of privacy or anonymity merely by being in a public place. Following Nader's publication of work highly critical of the General Motors Company, Nader claimed that GM tapped his telephone and hired call girls to gather incriminating information, in addition to "keeping him under surveillance in a public space for an

[14] *Katz v. United States*, Opinion of the Court.
[15] *Kyllo v. United States*, 533 US 27, Syllabus (2001).

unreasonable length of time." The New York Court of Appeals found

> A person does not automatically make public everything he does merely by being in a public place... On the other hand, if [Nader] acted in such a way as to reveal that fact to any casual observer, then it may not be said that the appellant intruded into his private sphere.[17]

The court recognized a difference between observation and the intrusion into one's "private sphere." More importantly, because the court also recognized that an invasion of privacy can occur in a public place there must also be an expectation of privacy in public spaces. By extending its interpretation on invasion of privacy as a tort, the Court discussed the liability that attaches to one who "unreasonably and seriously interferes with another's interest in not having his affairs known to others."

McIntyre v. Ohio Elections Commission

In McIntyre, the Supreme Court recognized the importance of anonymity as a type of speech and the role of anonymity in the public sphere. McIntyre recognized circulated pamphlets without printing her name or address, in violation of Ohio code prohibiting distribution of campaign literature lacking the same. Her estate brought suit against the Ohio code for infringing on her right to publish anonymously, a type of free speech protected by the First Amendment.[18]

The Supreme Court in 1995 decided that the prohibition of anonymous campaign literature abridges the freedom of speech. While the Ohio State Court argued the restrictions were "reasonable and nondiscriminatory" limitations to prevent fraud, libel, or false advertising, the Supreme Court found that the First Amendment protects all speech, both literary and political.

> The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible. Whatever the motivation may be, at least in the field of literary endeavor, the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment. [19]

More than simply a manifestation of First Amendment rights, the Court also felt it was critical to protect anonymity as an essential kind of public behavior.

> Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation – and their ideas from suppression – at the hand of an intolerant society.[20]

McIntyre provides the grounds upon which anonymity as a kind of public behavior can be protected.

---

[16] *Kyllo v. United States*, Opinion of the Court.
[17] *Nader v. General Motors Corporation*. 25 N.Y.2d 560, Opinion of the Court (1970).
[18] *McIntyre v. Ohio Elections Commission,* 514 U.S. 334, Syllabus (1995).
[19] *McIntyre v. Ohio Elections Commission*, Opinion of the Court.
[20] ibid

Indeed, if one's is guaranteed the right to speak anonymously in a public arena, then there must be a symmetrical right to remain anonymous in a public arena regardless of speech.

Right to Privacy

This 1890 Harvard Law Review article written by Samuel Warren and future Supreme Court Justice Louis Brandeis was written in response to the advances in the technological capabilities of cameras and invasive reporters. While trespass, assault, and libel had been recognized as injurious acts worthy of legal safeguards in the common law, invasive acts from the "enterprising press, the photographer, or the possessor of any other modern device for rewording or reproducing scene or sounds" did not warrant the same protection. The authors sought to define enforceable boundaries between the public and private life of individuals. Warren and Brandeis recognized an individual's "right to be let alone" as a personal freedom that is as much protected by the Constitution as free speech.

> It is like the right not be assaulted or beaten, the right not be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed. In each of these rights, as indeed in all other rights recognized by the law, there inheres the quality of being owned or possessed. [21]

"Right to Privacy" is a historic legal treatise not only because it argues the case for a freedom never explicitly mentioned in the Constitution, but because it call on the law to evolve in step with advances with technology. The authors chronicle the expansion of the law to protect individuals first from actual bodily injury, then to attempts to cause injury, then to nuisance, and beyond to the "corporeal property" to those "incorporeal rights issuing out of it and... the wide realm of intangible property" like those protected by patents and copyright.

> This development of the law was inevitable... Thoughts, emotions, and sensations demanded legal recognition, and the beautiful capacity for growth which characterizes the common law enabled the judges to afford the requisite protection.[22]

Forecasting his famous dissent in *Olmstead v. United States*, Brandeis developed an argument deriving from the First and Fifth Amendments that an individual inasmuch as he has a freedom of speech has a symmetrical freedom to not speak.

> The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others. Under our system of government, he can never be compelled to express them (except when upon the witness stand); and even if he has chosen to give them expression, he generally retains the power to fix the limits of the publicity which shall be given them. The existence of this right does not depend upon the particular method of expression adopted.[23]

The authors attempt to develop a legal framework to protect this right not as a contract, but as "rights as against the world." They deduce more obvious principles, like the protection of personal writings and other products of the intellect, as merely representations of an unstated right to privacy. To this end, they

[21] Warren, Samuel. Brandeis, Louis. *Right to Privacy.* Harvard Law Review 4, no. 5 (1890).
[22] ibid

propose that one's privacy can be as much subject to willful or negligent injury as those principles explicitly protected by law.

> If the invasion of privacy constitutes a legal injuria, the elements for demanding redress exist, since already the value of mental suffering, caused by an act wrongful in itself, is recognized as a basis for compensation... The remedies for an invasion of the right of privacy are also suggested by those administered in the law of defamation, and in the law of literary and artistic property, namely: (1) An action of tort for damages in all cases. Even in the absence of special damages, substantial compensation could be allowed for injury to feelings as in the action of slander and libel. (2) An injunction, in perhaps a very limited class of cases.[24]

The "Right to Privacy" was prescient argument on behalf of diminishing levels of privacy in the face of technological challenges. The positions and recommendations it makes are the same that we attempt to establish: while the private and public realms may be separable, an individual's expectations of privacy does not change when crossing such boundaries. This expectation and right is innate and understood from the body of rights protected by the Constitution.

Reno v. Condon

The 1994 Driver Privacy Protection Act regulated the sale of personal information to marketing companies. The personal information was provided by automobile owners to State departments of motor vehicles and included individual's names, addresses, telephone numbers, vehicle description, Social Security numbers, medical information, and photographs. The Attorney General of South Caroline filed suit alleging the DPPA violates the Tenth and Eleventh Amendments regarding federalism and division of power among the state and Federal governments.[25]

The Supreme Court in 1999 unanimously found that the DPPA "did not run afoul of the federalism principles" and was a proper exercise of Congressional authority to regulate interstate commerce.[26] The Court based its opinion on South Carolina v. Baker which substantiated the Federal government's role in regulating the activity of the State as database owners and operators, not controlling the State's "sovereign capacity to regulate their own citizens."[27]

This case did not develop an argument for protecting personal information from distribution. However, it did establish that personal information, as a commercially valuable commodity, was an article in interstate commerce and subject to Congressional authority. This case is the precedent upon which our proposed legislation will regulate both Federal and State activities involving sensors.

---

[23] ibid
[24] ibid
[25] *Reno v. Condon,* 528 U.S. 141, Syllabus (2000).
[26] *Reno v. Condon,* Opinion of the Court.
[27] Ibid

Olmstead v. United States

The Supreme Court upheld a decision that allowed Federal agents to wiretap the accused's phone line. Because the arguments for this decision, namely the trespass principle, were ultimately overturned in *Katz*, the dissenting opinions in this case are granted greater weight. Justice Brandeis who had previously written “Right to Privacy” presented a fascinating perspective on privacy and speech.[28]

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone -- the most comprehensive of rights and the right most valued by civilized man.[29]

Certainly the Founders depended upon privacy as a kind of security to advance the cause of liberty. In granting the many freedoms from government, they centered on the protection of individuals from the abuses of power by centralized governments. To this end, the concept of privacy underlies and unites these disparate protections.

> But "time works changes, brings into existence new conditions and purposes." Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet. [30]

While these founders could never have predicted the technological developments that would come to challenge their protections, they nevertheless built in protections against the expansion of centralized power in the Ninth and Tenth Amendments. The founders expected judges to exert discretion and allow the law to evolve in response to changes in technology.

Recommendation

The Supreme Court has recognized the existence of a penumbra of rights or implicit Constitutional protections. Because individuals have a reasonable expectation of privacy, even in public spaces, their anonymity should be protected from invasive searches by sensor technologies. The Congress has the authority and power to legislate how both the federal and state governments use collected personal information. While the legal understanding of anonymity in the public sphere has been developed, legislation is necessary to extend these protections implied in the Constitution into a comprehensive and enforceable law.

---

[28] *Olmstead v. United States,* 277 U.S. 438, Syllabus (1928).

[29] *Olmstead v. United States,* Dissenting Opinion.

[30] ibid

Sensor Technologies

We studied four types of sensors technologies: (in order of discussion) video surveillance, RFID, biometrics, and the Internet. We start with the more familiar video surveillance technologies that lie on the more passive side of the identification spectrum. We move on to RFID which is more active than video surveillance. One of the most active technologies to date is the biometrics, which we discuss after RFID. Finally we move from the physical world to the Internet to consider sensor technologies aboard on the Internet. Each survey of the technology shows concerns of privacy and anonymity through legislative background and case studies and makes overall recommendations that are incorporated into PAPA.

Video Surveillance

Video surveillance is the most recognized and widely used method of monitoring and recording public spaces. Closed circuit television (CCTV) systems transmit signals over a closed loop to a remote viewing location or group of users.[31] Currently, this is accomplished by collecting images with digital or analog video cameras, transmitting the images over cables, wireless transmitters, or the electronic networks like the Internet. Every advance in technology will allow images to be stored for longer periods of time, distributed to a larger group of users, and analyzed for more information. Given the potential in current and emerging technologies to invade an individual's expectation of privacy or anonymity in public spaces, current regulation does not sufficiently protection an individual's rights. This section will identify the concerns raised by video surveillance, the deficiencies of current legislation and regulations, and areas where policies could be improved to protect basic rights.

Analysis Framework

Our framework examines a sensor's human functional equivalent, degree of consent, pervasiveness, and identification potential in order to comparatively analyze the risk to anonymity posed by video surveillance technologies.

Human Functional Equivalent

The current technical capabilities of video surveillance would be akin to an individual in a public space taking copious notes on the observable aspects of the location, including appearances and actions of people. The individual does not necessarily recognize anyone but he observes patterns for individuals. These notes are then stored and can be easily copied and distributed to many recipients.

[31] Anna McCarthy. *Closed Circuit Television*. The Museum of Broadcast Communications. http://www.museum.tv/archives/etv/C/htmlC/closedcircui/closedcircui.htm

Consent

The only way to opt-out of video surveillance is to remain out of the sensor's field of view. However, it is impossible to know or see any boundaries to allow one to avoid monitoring and thus there is no opt-in/opt-out system in place for video surveillance. The public is rarely notified of the presence of video surveillance cameras, and individuals do not have a choice about whether their likenesses are captured with these cameras.

Pervasiveness

Video surveillance systems have been used for more applications over the past few years in response to both increased fears about terrorism and greater capabilities and features.[32] Video surveillance is used in security applications including: crime prevention and response; security of the property of private entities; security of individuals, including those who have a limited ability to take care of themselves; and a perceived feeling of security in the public. As Chicago Mayor Richard Daley stated, "cameras are the equivalent of hundreds of sets of eyes. They're the next best thing to having police officers stationed at every potential trouble spot."[33] Other uses of video surveillance include monitoring, such as that performed by transportation and highway departments to determine traffic flow.

Although no studies document the exact numbers of surveillance cameras in use nationally, some information is available on the prevalence of usage by specific entities in certain locations. In order to determine the extent of usage and hence the extent of potential anonymity concerns, we examine government and private use of surveillance systems.

Government Usage

Video surveillance deployment by government entities includes usage by law enforcement agencies, public transportation and transit systems, road and highway departments, public housing, and public schools.

In Boston, MA, hundreds of video cameras are operated and in use by government agencies. 200 cameras have been installed for the Big Dig project, 400 cameras are in use by the Massachusetts Port Authority, 27 by the Boston Transportation Department,[34] a classified number by the Massachusetts State Police, 100 by the MBTA, and 75 by the federal government.

Recently, preparations for the Democratic National Convention in July 2004 have led to an increase in video surveillance utilization, as the police department purchased and installed 30 cameras. In addition,

---

[32] Marcus Nieto, Kimberly Johnston-Dodds, and Charlene Simmons. "Public and Private Applications of Video surveillance and Biometric Technologies." California Research Bureau. March 2002.

[33] Fran Spielman and Frank Main. "City Plans Camera Surveillance Web", *The Chicago Sun-Times*. September 10, 2004. http://www.lexisnexis.com/

[34] John McElhenny. "Smile, you're on security camera." *The Boston Globe*. March 28, 2004.

during the Convention, video feeds from 75 cameras operated by the federal government were first linked to a surveillance network to monitor areas deemed high risk, such as the Central Artery, City Hall Plaza, and the FleetCenter. The Department for Homeland Security monitored this network at stations in Boston and Washington, D.C. While non-federal cameras did not share a similar networking system, law enforcement officials did arrange to share collected images to respond to emergencies. [35]

In 1995, St. Petersburg/Tampa Bay, FL installed video surveillance equipment in Ybor City, a pedestrian mall that includes many clubs, restaurants, and stores. In 2001, facial recognition technology was added to the existing system. This biometric technology was used by police to compare faces of individuals in Ybor City to 30,000 images from a database that included wanted criminals and runaways. Such technology represents one of the ways that video surveillance has an increasing ability to identify individuals in public spaces. However, due to its limited effectiveness, facial recognition was discontinued by the police department in 2002.[36]

The Chicago Police Department currently has access to live footage from 2000 surveillance cameras throughout the city, in areas controlled by the Chicago Transit Authority, Chicago Housing Authority, and Chicago public schools. Under a new plan instituted by Mayor Richard Daley, 250 cameras will be added to the existing system by early 2006, along with computer software capable of monitoring suspicious behavior. The software would be able to highlight images of individuals engaged in behavior such as turning in circles aimlessly or leaving a package and walking away from it. Thirteen employees at a 911 call center will monitor the cameras continuously, such that a telephone call to 911 would allow the call-taker to view the camera closest to the scene and direct police and firefighters accordingly.[37]

Private Usage

Private institutions were pioneers of video surveillance; banks first began using CCTV in the 1960s. Today, video surveillance is used by retail stores, parking terminals, casinos, nursing homes, and many other private entities. Although statistics are less readily available for private CCTV usage, it is possible to form an idea of their prevalence. FleetBoston, just one financial institution, uses video surveillance in all 427 Boston-area ATMs and 71 branches. In addition, civil liberties groups such as the New York City Surveillance Camera Project have performed unofficial counts of surveillance cameras in public areas. This group has located 2,397 video cameras in Manhattan, of which 2,117 are private.[38] The numbers indicate that the vast majority of video surveillance is utilized by private entities.

---

http://www.lexisnexis.com/

[35] Ralph Ranalli, and Rick Klein. "Surveillance targeted to convention." *The Boston Globe*. July 18, 2004. http://www.lexisnexis.com/

[36] Brady Dennis. "Ybor Cameras Won't Seek What they Never Found." *St. Petersburg Times*. August 20, 2003. http://www.lexisnexis.com/

[37] Fran Spielman and Frank Main. "City Plans Camera Surveillance Web." *The Chicago Sun-Times*. September 10, 2004. http://www.lexisnexis.com/

[38] New York City Surveillance Camera Project. Project Information. http://www.mediaeater.com/cameras/breakdown.html

At times, private sector usage of surveillance cameras is not voluntary. In January 2004, the Superior Court of Orange County, California, upheld an ordinance of the City of Garden Grove to require cybercafe owners to maintain video surveillance and keep the gathered images for 72 hours, due to rising gang-related violence in cybercafes.[39] Thus, the rising prevalence of video surveillance has led to a requirement instituted by a government entity for private sector usage. Although this legislation and judicial ruling is justifiable, it increases the reasons for private entities to install video surveillance, and thus also increases the number of video cameras present in public spaces.

Identification Potential Spectrum

Presently, video surveillance systems are limited in their ability to identify individuals. This can be determined by analyzing the current technology development using our identification potential spectrum, with the categories of collection, storage, processing, and distribution. Collection of images by video surveillance systems is accomplished by either analog or digital video cameras. Cable or wireless transmitters then send the images to a central monitoring location for storage. Personnel may monitor incoming images for suspicious behavior, recognized criminals, or limited comparisons with databases. The poor enforcement of the few regulations on image distribution raises significant privacy concerns and risk to public anonymity.

Because the sensor activity of video surveillance systems features little processing, analysis, or distribution compared to current applications emphasizing collection and storage, video surveillance is located on the passive side of the identification potential spectrum. Unless the viewer knows the individual or has probable cause to determine the identity of an individual (as in the case of those who run red lights and are caught by red-light cameras), it is difficult to identify an individual or his personal information. However, emerging technologies that will enhance the ability to collect, process, and distribute images, will expand the ability to link a captured image to an individual's identity.

Collection and Storage

Sensor technology in video surveillance systems has incorporated smaller sizes, increased range, better resolution, higher zoom, and improved low-light monitoring features. These advances have an indirect effect on video surveillance's place in the identification potential spectrum. Sensors generating enhanced images are able to present a more accurate record of an individual's face and the environment around the individual which provides a more accurate link between an individual's identity and location.

Processing

Emerging technologies in information processing and analysis have the potential to identify individuals. Facial recognition and increased database linkages provide a vital bridge between location data and

[39] *Vo v. City of Garden Grove,* 115 Cal.App. 4th 425, 2004 Cal. App. Lexis 116.

personal information, presenting possible infringement of the right to anonymity.

One widely-used algorithm for present facial recognition systems uses a series of landmarks, or nodal points, such as the distance between the eyes or the width of the nose, on the human face to identify individuals. The software uses images captured by surveillance cameras and measures these nodal points, then creates a unique numerical code, or faceprint. These faceprints can be matched to others in a database.[40]

Facial recognition is limited in its ability to identify individuals in a crowd. Recently, facial recognition technology has failed in some tests for picking faces out of a crowd. In 2002, the ACLU released information from the Tampa Police Department operator logs, showing a high number of false positives generated by the FaceIt software manufactured by Visionics.[41] The National Institute of Standards and Technology also conducted tests of facial recognition technologies with their FERET Evaluation Methods. Their results indicated that variables such as changing illumination and changing facial position greatly affect performance of the software.[42] In addition, shortly after September 11th, officials at Logan International Airport in Boston tested facial recognition technology developed by Visionics and Lau Technologies. Two checkpoints were set up that experienced similar amounts of traffic. Faceprints of individuals traveling through each checkpoint were matched against two databases: one of suspected terrorists, and a second, control group of police officers and maintenance crew with no prior offenses. The technology failed to provide accurate identification, and was not implemented at Logan Airport.[43]

Despite the current limits of facial recognition technology, it is currently being used in casinos to pick out cheaters, or card counters, at blackjack tables. Some states have used the technology to check for those who have obtained multiple driver's licenses.[44] Technological advances and refined facial recognition software could reduce and possibly eliminate the current problems of identifying individuals in a crowd, thus creating a link between one's appearance and one's personal information. This emerging technology has the potential of shifting video surveillance to the active side of the passive-active spectrum.

Another emerging processing technology that affects the ability of video surveillance to personally identify individuals is that of increasingly linked databases. Some of these technologies are produced by software firms in order to combat terrorism. Programs such as NORA (developed by SRD) and CopLink (KCC) search through databases of different agencies and identify relationships between entities such as mug

---

[40] Kevin Bonsor. "How Facial Recognition Systems Work." *Howstuffworks*. http://people.howstuffworks.com/facial-recognition.htm

[41] Jay Stanley and Barry Steinhardt. "Drawing a Blank: the failure of facial recognition technology in Tampa, Florida." *An ACLU Special Report*. January 3, 2002.

[42] Phillips, P. Jonathon, and others. National Institute of Standards and Technology. "An Introduction to Evaluating Biometric Systems." IEEE. February 2000.

[43] Chief John DiFava, Interview, 17 November 2004.

[44] Barnaby J. Feder "Technology Strains to Find Menace in the Crowd." *The New York Times*. May 31, 2004. http://www.lexisnexis.com

shots, locations, weapons, vehicles, and addresses, combining the information in these databases for law enforcement and private sector usage. [45]

The federal government also has programs in place to exchange information between different federal, state, and law enforcement agencies. The Department of Homeland Security has expanded its computerized information network, known as the Joint Regional Information Exchange System (JRIES), to all 50 states and 5 territories. This system would allow users to send photos, maps, streaming video, and other information.[46] Individual states have also made efforts to facilitate the collection and sharing of information. For example, the Pennsylvania Criminal Intelligence Center was created within the PA State Police to give law-enforcement personnel access to Pennsylvania and interstate criminal information databases.[47] In May 2004, an intelligence center located near Albany, NY, began operation and provided tens of thousands of law enforcement officers in New York and Vermont with classified FBI counter-terrorism databases.[48]

One concern raised by database linkage is that the system can be compromised, that an individual without authorization can hack into the system and obtain personal information on many individuals. Even without access to systems such as JRIES, a person with access to a program such as NORA could hack into separate databases and combine personal information. In addition, entities that are authorized to view these databases may abuse these systems. Breaches of privacy and anonymity of individuals, such as collecting, storing, and distributing information of individuals for irrelevant purposes, could occur.

These two emerging technologies: facial recognition and increased database linkages provide a vital bridge between location data and personal information, presenting possible infringement of the right to anonymity.

Distribution

Advances are also being made in technologies involved in distribution of images. One such development involves the Internet – the emergence of IP Surveillance. IP Surveillance refers to the technology that allows for viewing of collected images via LAN or the Internet by assigning IP addresses to different surveillance cameras. It is possible to restrict access to authorized individuals, or the images could be broadcast over the Internet. This leads to the increased distribution of collected images, and thus an increased ability for many to identify an individual in a certain location.

---

[45] Jesus Mena. "Homeland Security as Catalyst." *Intelligent Enterprise*. July 2004. http://www.intelligenteai.com/showArticle.jhtml?articleID=22102265

[46] "Terror-fighting network touted." *The Washington Times*. February 25, 2004. http://www.lexisnexis.com/

[47] "State Police, PCCD Announce Changes to Improve Collection, Sharing of Information by Law Enforcement Agencies." Pennsylvania State Police Press Releases. August 27, 2003. http://www.psp.state.pa.us/psp/cwp/view.asp?A=11&Q=170383

[48] David Johnston. "Terror Data to be shared at New Center Near Albany." The New York Times. May 25,

The increased pervasiveness of surveillance cameras, inability to opt-in/opt-out of the system, and the emerging abilities to link personal information with location data are changing the scope and magnitude of the human functional equivalent of video surveillance. Instead of one individual taking copious notes, these emerging factors lead to the analogy of many individuals. These individuals are sometimes invisible, or able to zoom in and read the letter in one's hand, or be in many places at once. What can one do to limit the number of recipients of these notes? How can one limit the amount of personal information these notes reveal?

Human Functional Equivalent	Individual taking notes on observable aspects of a public space
Consent: Opt-in or Opt-out	Little to None
Pervasiveness	Widespread and increasing
Personally Identifiable	Presently limited

Table 1: Summary of Application of Analysis Framework in evaluating anonymity and privacy concerns in video surveillance.

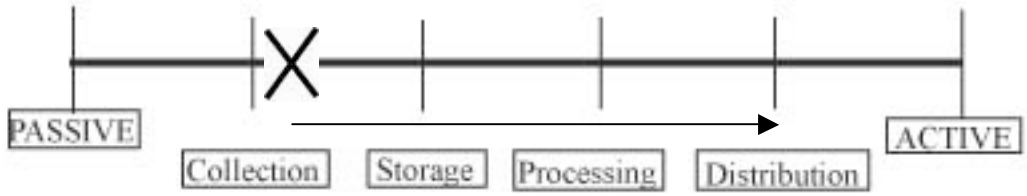

Figure 1. Identification Potential Spectrum. Emerging technologies with video surveillance will shift its place on the identification potential spectrum to the active side.

Values

These developments in collection, processing, and distribution technologies have the potential to shift the location of video surveillance on the identification potential spectrum – that is, to link location data with personal information (Figure 1). Both the current passive technology and the future, more active technology give rise to a need to protect the basic rights to anonymity and to self personal information.

Case studies

The framework demonstrates the expanding applications of sensor technologies. We present three case studies demonstrating specific instances of the abusive potential for video surveillance. The 2001 Super Bowl in Tampa, Florida; inappropriate use of traffic cameras by state troopers in Tuscaloosa, Alabama; and the wrongful distribution of suicide footage by government programs highlight concerns with the collection, storage, processing, and distribution of images by contemporary video surveillance techniques.

2004. http://www.lexisnexis.com/

Super Bowl XXXVI

The 2001 Super Bowl in Tampa, Florida, was the first large-scale usage of facial recognition technology in the United States. At the turnstiles of Raymond James Stadium, the face of each individual who entered the stadium was captured by a video camera. The images were then sent to a control room inside the stadium, where facial recognition software, provided by Viisage Technology Inc., sought to match the facial signatures with digitized facial data of a criminal database.[49] No arrests were made using the technology, although one match was made: that of a ticket scalper, who vanished into the crowd. Law enforcement officers noted that this technology is no more invasive than video surveillance in a convenience store,[50] and that images were not kept permanently.[51] There was no public notification that these technologies would be used, and fans were unaware of the surveillance until it was reported by the media.

Most objections to the Super Bowl incident involved the lack of notification. As the ACLU noted,

> While similar surveillance systems are used at convenience stores, shopping malls and schools across the country, citizens are generally informed that the area is under surveillance and of the camera's whereabouts, unlike the thousands of sports fans who entered Raymond James Stadium for the big game.
>
> As they entered at turnstiles, fans had no clue their faces were being silently digitized and matched up against the mug shots of criminals and terrorists, or that they could be questioned or detained by officers.[52]

In general, in order for individuals to properly control their own information, it is necessary for them to know where, when, and how data is collected. However, in this case, the crowd was scanned for potential terrorists – a need that would be undermined by public notification of surveillance use. As Tampa police spokesman Joe Durkin noted, "Had the system been able to identify a known terrorist and had Tampa police been able to stop him, this tool would have been invaluable."[53] Use of video surveillance to identify potential terrorists is within the scope of the Tampa police department, and the department adhered to this usage throughout the game. Beyond the issue of notification, law enforcement showed restraint in this case. The value of anonymity was not breached, because information about individuals who were not suspected criminals were not retained. Thought images were captured on a camera, the public's anonymity was not violated. Thus, because restraint was used in this situation, and because usage of video surveillance was not beyond the scope of the law enforcement agency, the 2001 Super Bowl demonstrated a legitimate usage of the technology.

---

[49] Robert Trigaux. "Cameras Scanned Fans for Criminals." *St. Petersburg Times*, Jan 31, 2001. http://www.lexisnexis.com/

[50] Peter Slevin. "Police Video Cameras Taped Football Fans." *The Washington Post*, February 1, 2001. http://www.lexisnexis.com/

[51] Trigaux, "Cameras Scanned Fans for Criminals."

[52] ACLU. "ACLU Calls for Public Hearings on Tampa's 'Snooper Bowl' Video Surveillance". Press Release. February 1, 2001. http://www.aclu.org/Privacy/Privacy.cfm?ID=7117&c=130

[53] Slevin, "Police Video Cameras Taped Football Fans."

Tuscaloosa State Police

A contrasting example involves the unsavory use of video surveillance sensors in Tuscaloosa, Alabama in September 2003. A state trooper posted at Skyland Boulevard, near the University of Alabama, used a traffic camera to zoom in on women's breasts and buttocks. The images were broadcasted on a local cable channel and the woman was arrested for exposing her breasts to the camera. In response, the Department of Public Safety and the state troopers lost the right to operate video cameras on the streets of Tuscaloosa, although they would still be able to see video footage from about 20 cameras. The agreement also stipulated that the DPS would share the details from an inquiry into the incident, including any action taken. The City Transportation Director said that he believed the employee guilty of the improper usage had been transferred. However, the report was not made public, nor was a copy of the final disciplinary action released.[54]

This case illustrates one example of a government agency using surveillance cameras for reasons beyond the proper scope. Clearly, the Department of Public Safety was not authorized to use surveillance cameras for viewing specific parts of women's bodies. The fact that such conduct occurred suggests that troopers were not properly trained and/or supervised for traffic camera usage. In addition, the subsequent broadcast on a cable channel shows inappropriate distribution of video footage. This distribution caused the women to lose their right to anonymity, or their right to conduct business without disturbance of their personal solitude. Finally, it is difficult for the community to determine whether proper measures had been taken to prevent such an incident from occurring again. Neither the report by the Department of Public Safety nor the final disciplinary action was made available, and the public does not have a clear knowledge of whether their public anonymity and privacy would be intruded upon again.

Paris Lane Suicide

A third example involves a suicide in a New York City housing project. On March 16, 2004, rapper Paris Lane used a handgun to kill himself in a lobby of a Bronx housing project. The act was caught on a police security video camera, and subsequently appeared on a website, Consumption Junction, dedicated to violent and pornographic images. The website labeled the footage as "Introducing: The Self-Cleansing Housing Projects." The foster mother of the diseased, Martha Williams, had been notified by others of the existence of the video, and afterwards informed C. Virginia Fields, the Manhattan borough president.[55] It was determined that a police officer in the Video Interactive Patrol Enhanced Response (VIPER) unit emailed the suicide video to a friend, who then forwarded it to other individuals until it appeared on the website.[56] In response, Police Commissioner Ray Kelly required NYPD captains to make at least one visit

[54] "Troopers to be hands-off with Tuscaloosa traffic cameras". *Associated Press*. January 15, 2004. http://www.lexisnexis.com/

[55] Shaila K. Dewan. "Video of Suicide in Bronx Appears on Shock Web Site." *The New York Times*. April 1, 2004. http://www.lexisnexis.com

[56] Murray Weiss. "Suicide Video Shock – Linked to L.I. Cop". *The New York Post*. April 6, 2004. http://www.lexisnexis.com

each eight-hour shift to every VIPER unit under their command.[57]

This example shows the inappropriate distribution of footage from police surveillance cameras. Due to the advancement of technology, it is possible, and increasingly simple, to distribute digital images via the internet to a larger network of people. However, Mr. Lane's privacy was invaded by this distribution. He lost the right to control his own personal information, about his suicide in a particular location, since many unauthorized individuals viewed this act. While it is good that the NYPD re-evaluated the VIPER program, such a breach of Lane's rights is not warranted.

Geoffrey Peck Suicide

Finally, a fourth case shows a similar event in Europe that came under the jurisdiction of the European court of Human Rights. On August 20, 1995, Geoffrey Peck, was walking through the streets of Brentwood, UK with the intent of suicide. He stopped at a central junction in the center of the city and faced the traffic with a kitchen knife in his hands. Unknown to him, his movements were caught by a traffic camera installed by the Brentwood Borough Council. The camera operator alerted police to the presence of an individual with a knife, and police arrived on the scene, took the knife from Peck, gave him medical assistance, and brought him to the police station. On September 14, 1995, the Brentwood Borough Council authorized the release of regular press features of the CCTV system. Subsequently, images from Peck's attempted suicide were released to and used by the CCTV News (a publication by the Council), the Brentwood Weekly News, the Yellow Advertiser, Anglia Television, and "Crime Beat" (a program on BBC national television). The Council had verbally required that the programs mask Peck's identity, although the masking was done inadequately. Peck's acquaintances still had the ability to identify him, and Peck found out about these distributions. He made a number of media appearances to speak out against the dissemination of the footage, and also applied to the High Court, arguing that the Council's disclosure had no basis in law. The High Court disagreed with Peck, stating that although Peck did suffer an invasion of privacy, it was reasonable for the Council to distribute the footage to demonstrate the capabilities of CCTV. [58]

However, Peck appealed the High Court's decision to the European Court of Human Rights. This court was set up in 1959 by the European Convention on Human Rights of 1950 in order to maintain and realize human rights and fundamental freedoms.[59] In January 2003, the court concluded that the actions of the Council violated Articles 8 and 13 of the European Convention, which state that there is a right to respect for private and family life, and that there is a right to an effective remedy. Although the court accepted that video surveillance can be a capable means of crime reduction, it also noted that the

---

[57] Philip Messing and Murray Weiss. "Top Cops Eye Video Villains." *The New York Post*. June 8, 2004. http://www.lexisnexis.com/

[58] *Peck v. United Kingdom*. The European Court of Human Rights (Fourth Section). Strasbourg. 28 January 2003.

[59] European Court of Human Rights. *Historical background, Organisation and procedure*. http://www.echr.coe.int/Eng/EDocs/HistoricalBackground.htm September 2003.

Council had failed to seek Peck's consent, to mask his identity effectively before distributing the footage, and to create written contracts with the media programs to ensure that Peck's identity was masked. Due to these lapses, the Council had breached Peck's right to privacy.[60]

The privacy issues brought up by Peck's case are similar to those of the Lane suicide video. However, because of legal proceedings in Europe based upon European legal protection of the right to privacy, Peck was remunerated for his loss of privacy, and the courts determined that the Council had breached this right through distribution of video surveillance footage. Such judicial ruling unequivocally sets forth the privacy rights which may not be violated with video surveillance usage.

These four cases demonstrate instances of possible violations of the rights to anonymity and to self-information. With current technology, such violations can occur when collection or distribution of images is done improperly. Advancement of video surveillance technologies in the categories of collection, processing, and distribution raise the possibility of further violations of privacy.

Current Legislation and Guidelines

It is important to determine the extent to which privacy rights in relation to video surveillance are protected by current legislation, judicial rulings and guidelines. There are both federal and internal guidelines to video surveillance usage. Most guidelines are in relation to law enforcement usage of surveillance cameras, though the private sector seems to enjoy more widespread usage of these cameras.

Federal Guidelines

There are three institutional guidelines for video surveillance usage: Department of Justice (US DOJ) Criminal Resource Manual 32 drafted in October 1997; the 1999 American Bar Association Standards; and the 2000 Security Industry Association CCTV guidelines.

The US DOJ Criminal Resource Manual 32 defines video surveillance as “the use of CCTV to conduct visual surveillance of a person or place.” It goes on to summarize Supreme Court cases that specify that video surveillance is not covered by Title III, also known as the Wiretap Act (1968). Instead, it is governed by the Fourth Amendment. Thus, under the Fourth Amendment, if a reasonable expectation of privacy exists, a search warrant is needed to use video surveillance. This search warrant would need to demonstrate: probable cause that the surveillance will obtain evidence of a federal crime; alternative investigative methods have failed, or appear too dangerous or unlikely to succeed; steps taken to minimize surveillance; a description of the monitored location; a duration of the authorization that is no longer than 30 days; and if known, the names of the surveilled individuals.[61]

---

[60] *Peck v. United Kingdom*

[61] *U.S. Department of Justice Criminal Resource Manual* No. 32, Title 9-618. “Video Surveillance – Use of

The American Bar Association (ABA) drafted standards for law enforcement usage of video surveillance. General considerations given by the ABA include the stipulations that the subjects of surveillance should not be arbitrarily or discriminatory selected, that the scope should be limited, that the technique should only be used for doing "what it purports to do", that notice should be given when appropriate, that disclosure of obtained information should only be permitted for lawful purposes, that protocols should be in place to maintain and dispose of records, and that law enforcement agencies should develop written instructions regarding surveillance usage. The ABA standards indicate that surveillance cameras can be used when it would not monitor private activities and when it will be likely to achieve a "legitimate law enforcement objective". When usage of surveillance cameras is needed for deterrence of crimes, rather than investigation of criminal offenses, the public should be notified of the location and technical capabilities of the camera, and that there should be opportunity for public comment before installation and during usage.[62]

The Security Industry Association (SIA) has its own guidelines for CCTV usage by law enforcement. The SIA is an international trade association with over 450 members that manufacture, distribute, and install electronic and physical security technology. In partnership with the International Association of Chiefs of Police (IACP) and National Sheriffs Association (NSA), it drafted a series of guidelines to law enforcement on use of non-court ordered overt surveillance, or surveillance of which a reasonable person would be aware. The guidelines suggest that personnel who use CCTV should be trained, closely supervised, and disciplined for breaches of protocols; that initial and ongoing needs assessments should be conducted; that information obtained should be used only for safety and law enforcement purposes and stored for "an appropriate time period"; that CCTV observation of residential areas should limit the view to that of the naked eye of an officer on the site; that law enforcement agencies should seek input from the community before CCTV implementation or expansion, and that a periodic system review or audit should be performed. The guidelines also list a series of legitimate CCTV applications in public areas for purposes such as protection of people and property, monitoring of access control systems, and traffic regulation or control.[63]

Internal Guidelines

Internal guidelines for state and local agencies are not always publicly available or applicable to all possible privacy breaches. One exception to this includes the set of guidelines of the Metropolitan Police Department (MPD) of Washington, D.C., which is the most tightly regulated CCTV system in the country,[64] and adheres to the standards set by the American Bar Association.

Closed-Circuit Television (CCTV)".

[62] Criminal Justice Section, American Bar Association. "Electronic Surveillance: Part B: Technologically-Assisted Physical Surveillance" 1999. http://www.abanet.org/crimjust/standards/taps_blk.html

[63] Chace, Richard W. *An Overview on the guidelines for Closed Circuit Television (CCTV) for Public Safety and Community Policing*. Security Industry Association. 2000.

[64] *CCTV – Policy and Procedures*. Metropolitan Police Department. http://mpdc.dc.gov/info/comm/CCTV_policy.shtm. Accessed 9 December 2004.

On November 7, 2002, the District of Columbia Council passed regulations guiding the MPD's use of video surveillance. These regulations, summarized below, offer a reasonable example of a privacy policy for video surveillance sensors in public spaces.

For collection, the system is only activated during major events or emergencies. An MPD official at the rank of lieutenant or higher will monitor all CCTV use. There are no audio capabilities with the CCTV system. Operators of the CCTV will not target or track individuals arbitrarily or based on race, gender, ethnicity, sexual orientation, disability or other such classifications protected by law. Cameras will not focus on hand bills, flyers or other materials distributed or carried as per the First Amendment.[65]

Recording of video images only occurs upon authorization of the Chief of Police. Unless there is evidence of necessity of court usage, images are stored for 10 business days, and then destroyed. [66]

In terms of processing, the system does not use face-recognition or other biometric technologies. [67]

The MPDC will notify the public about the capabilities and uses of the CCTV system, including the posting of signs indicating where the cameras will be deployed. The Department will provide regular reports on CCTV usage and will seek public comment on any proposed expansion of the network. Unauthorized use or misuse of the CCTV system will result in disciplinary action. The MPDC's Office of Professional Responsibility will conduct at least quarterly audits to ensure compliance.[68]

Concerns

Although these policies provide a basis for the protection of privacy, there are also concerns present with the current state of legislation. These concerns include the lack of universality, transparency, and enforcement in guidelines, and the subsequent insufficient protection of the right of anonymity and the right to self-personal information.

Current video surveillance guidelines are not universal. Each agency is free to create its own policies for usage. This leads to discordant guidelines practiced by different agencies, such as the extremely strict rules of the Washington D.C. MPD and the less stringent guidelines of other agencies, apparent in the case studies that violate personal privacy. Discordant guidelines lead to unequal protection of rights among different locales. Thus, the protection of personal anonymity and privacy are unequal in different areas in the United States.

---

[65]Ibid.
[66]Ibid.
[67]Ibid.
[68]Ibid.

A second issue is raised by the lack of transparency and enforcement in video surveillance guidelines. With the exception of the Washington D.C. Metropolitan Police Department, the locations of surveillance camera usage are not publicly known. Efforts by the New York Surveillance Camera Players and the NYC Surveillance Camera Project have mapped the locations of video camera usage in public places, but these maps are not comprehensive and take much effort to keep current. In addition, many of the proceedings dealing with abuses of video surveillance systems are not publicly shared, as illustrated by the Tuscaloosa state troopers case and the Paris Lane suicide case. Also, both these cases show the limited resources of individuals in dealing with improper usage of video surveillance. Because there is little enforcement of guidelines, the public has little recourse when rights are violated.

Current regulations cannot stop abuses, such as those detailed in the case studies, from violating the right of anonymity and the right to self personal information. As stated in the Values section, the right of anonymity is the right to conduct business without government intrusion or intrusion on personal solitude. Such a right is breached when images are collected for arbitrary reasons that do not relate to the reason for video surveillance installation. One's right to control his or her personal information can currently be impaired when footage is distributed to agencies or entities without authorization of the individual. In addition, as technologies such as facial recognition and database linkage increase in effectiveness and proliferate, there is a possibility that personal information such as credit history, Social Security number, or criminal history can be distributed to agencies or entities without authorization.

Despite the attempts at regulation by organizations like the American Bar Association and the Security Industry Association, these policies cannot protect the public's rights because they are neither universal nor enforced. Values such as the right to anonymity and the right to self information have been breached in the case studies because there is limited protection. Our legislation, PAPA, seeks to address the deficiencies of current legislation by protecting these rights.

Policy Recommendations

Due to the inadequacy of current policies to protect individual rights in video surveillance, some recommendations for policy follow.

PAPA seeks to protect the right of anonymity. This is especially important with government agencies, as the right of anonymity specifically tries to prevent government entities from intruding upon individuals. Therefore, government agencies must be able to provide clear statements of the goals of surveillance and the necessity of surveillance to the public. Usage of surveillance should not deviate from these goals, preventing acts such as the misuse of traffic cameras by the Tuscaloosa, Alabama state troopers. In addition, there should be no retention of personal information of those individuals who are not central to the purpose of the agency. For example, law enforcement organizations should not keep personal information of those who are not suspected of wrong-doing.

The right to self personal information is also protected by PAPA. In order for individuals to know when this right could be intruded upon by video surveillance usage, it will be necessary for both government agencies and private entities to provide notice of surveillance camera usage. However, it will not be necessary for law enforcement to provide such notice when the purpose of surveillance camera usage is for events or emergencies in which there is suspected criminal activity and the security of the public is in danger, such as the suspicion of terrorist activity at the Super Bowl. This exception is in place to ensure that law enforcement can still protect public safety. In addition, images should not be distributed except for law enforcement purposes. The law enforcement agency must have probable cause for requesting such footage, and either a court order or written request signed by a ranking officer will be needed.

The last recommendation for PAPA centers upon enforcement. For government agencies, a central regulatory body should be set up, if it is not in existence already, to oversee surveillance system operation. A regular auditing process should be instituted to ensure that guidelines are adhered to. For private entities, individuals will retain the ability to bring legal suits when their rights have been abridged. These mechanisms will ensure that PAPA is followed, and provides recourse for individuals should their privacy be violated.

Conclusion

As technologies advance and the pervasiveness of video surveillance increases, its ability to identify and locate individuals will also increase. Because current video surveillance guidelines do not adequately protect individual privacy rights, there exists a need for legislation to ensure that these rights are not violated. In this section, policy recommendations were proposed to protect the right of anonymity and the right to self personal information, as well as to provide sufficient enforcement mechanisms. It is hoped that these recommendations will be utilized to prevent erosion of privacy rights due to the current and future abilities of video surveillance systems to identify individuals.

RFID

Radio Frequency Identification (RFID) is a method in which data is stored and transmitted remotely using the radio frequency associated with RFID tags.[69] A transceiver sends a radio-frequency query to the tag, and the transponder replies by broadcasting identifiable information. RFID devices can be active or passive in design. Active RFIDs require the transponder to have an internal power source of some sort. Passive tags, on the other hand, draw their power inductively from the RF energy transferred from the reader to the tag.[70] Because of this difference in design, active RFID transponders are capable of accepting low-level signals and broadcasting high-level signals back to the transceiver, and then have a

[69] "RFID." Wikipedia. http://en.wikipedia.org/wiki/RFID
[70] "Part 1: Active and Passive RFID: Two Distinct, But Complementary, Technologies for Real-Time Supply Chain Visibility." Auto-ID Center. http://www.autoid.org/2002_Documents/sc31_wg4/docs_501-

range of tens of meters. Meanwhile passive tags require a strong signal but can only respond with a weak one, and thus they have a smaller range going from 10 millimeters up to 5 meters. Because passive RFID tags are cheaper, often costing as little as $0.40, they represent the majority of RFID devices in the market today and are increasingly used in high-volume scenarios, such as merchandise inventory tags.[71]

The earliest use of RFID was by the British during World War II. Royal Air Force planes were fitted with RF tags to so that, when flying back to their bases, the planes could be distinguished from inbound German ones. Named Identification Friend or Foe (IFF) and still used today in modern air warfare, the system automatically responded to electromagnetic transmissions with RF pulses to distinguish itself from the enemy.[72] Later that same decade in 1945, the Russian inventor Leon Theremin created an RFID espionage tool for use by the Soviet Government. The inductive device was embedded on a plaque and presented to the American Ambassador in Moscow by Russian schoolchildren. It was a passive tag that, when remotely powered, would broadcast audio from within the Ambassador's office to the transponder's listener, and without ever needing a power source it had in indefinitely long life.[73]

Case Studies

The best way to go about understanding the need for privacy and anonymity legislation with RFID technologies is to look at case studies. A summary of RFID technologies in the framework is shown in Table 2. Figure 2 places RFID on the identification potential spectrum. Case studies we looked into are VeriChip, RFID in retail use, and Electronic Toll Collection systems.

VeriChip

An example of a passive RFID device is the VeriChip implantable tag.[74] Created by Applied Digital Systems (hereafter referred to as ADS), the chip is the size of a grain of rice and is generally implanted below the arm, in the triceps region, or in the hip. The implantation is a short, outpatient surgery, and the VeriChip is coated with BioBond, which allows it to adhere to local tissue but insulate it from the body. ADS believes that in the future the device will prove to be an effective way of "providing secure tamperproof identification for a variety of medical, financial security & other application".[75] Slowly, VeriChips are being adopted in some parts of the world in various security and emergency identification scenarios. In October of 2002, the US Food and Drug Administration ruled that the VeriChip could not be considered a regulated device in regards to its financial, security, safety, or personal identification applications, because there are no regulations or legislation governing the use of the VeriChip. Instead, the FDA deemed that it could only regulate the VeriChip in its applications of healthcare information.[76]

520/520_18000-7_WhitePaper.pdf

[71] Wikipedia

[72] "Identification Friend or Foe." Wikipedia. http://en.wikipedia.org/wiki/Identification_friend_or_foe

[73] "Leo Theremin." Wikipedia. http://en.wikipedia.org/wiki/Leon_Theremin

[74] VeriChip. http://www.4verichip.com

[75] Applied Digital Systems. http://www.adsx.com

[76] "VeriChip," Wikipedia. http://en.wikipedia.org/wiki/Verichip

VeriChip Health Information Microtransponder System

On 13 October 2004, the FDA approved the use of VeriChip for medical identification purposes, and on 10 November 2004, ADS signed a distribution deal with Henry Schein, the largest supplier of healthcare products in North America and Europe. Each VeriChip Health Information Microtransponder System contains a unique 16-digit verification number, and when scanned by a registered healthcare provider, it transmits the number to the reader, and the reader in turn connects via "secure, password protected web access"[77] to ADS's Global VeriChip Subscriber[78] Registry (hereafter referred to as GVS) and provides the healthcare professional with subscriber-supplied information. The information collected generally contains blood type, known allergies, prescribed drugs, patient's ailments, and possibly contact information for the patient's physician. The hope is that, by having this information readily available regardless of the physical condition of the patient at the time of an emergency, emergency workers can work faster and more effectively to save the patient's life. It also alerts the patient's physician and family of his location and that an emergency situation has occurred.[79]

VeriChip Internationally

Solusat, VeriChip's Mexican distributor, is marketing VeriChip as a way of tracking and identifying children if they are abducted or missing. Mexico's National Foundation of Investigations of Robbed and Missing Children backs the service, citing that an estimated 133,000 Mexican children have been abducted over the past five years.[80] The idea behind VeriKid is that there will be walk-through VeriChip readers at public places where children are likely to go, such as malls, bus terminals, parks, and movie theaters. A VeriKid-equipped child, flagged in the GVS, walking through a detector in these areas will alert authorities to the child's location.

A program in Mexico City has tagged 170 police officers.[81] These VeriChips act as access control and allow the tagged officers access to secure police databases and sensitive materials.[82] Additionally in Spain, the Baja Beach Club in Barcelona uses VeriChips to identify their VIP customers, making it the first business in the world to use the technology for both access and payment options.[83] Customers can have the implantation done at the club, and as soon their information is entered into the club's database, the customer can enter restricted VIP areas and make payments without ever having to carry a wallet or ID badge around the resort.

---

[77] VeriChip website
[78] GVS Registry Login. https://gvsregistry.4verichip.com
[79] Wikipedia
[80] "Tracking Junior With a Microchip." *Wired News*, 10 October 2003. http://www.wired.com/news/technology/0,1282,60771,00.html
[81] Wikipedia
[82] Sean Coughlan. "Security Under the Skin." *BBC News World Edition*, 15 October 2004. http://news.bbc.co.uk/2/hi/uk_news/magazine/3742684.stm
[83] Sherrie Gossett. "Paying For Drinks With Wave of the Hand." *World Net Daily*, 14 April 2004. http://worldnetdaily.com/news/article.asp?ARTICLE_ID=38038

Future Use

Currently, ADS also markets VeriTrak and DigitalAngel. VeriTrak allows company owners to track their inventory and employees by attaching radio antennas to them. However, ADS plans to incorporate VeriChip into VeriTrak and provide an easier way for employers to track their employees. This system will enable companies to track where employees are within the VeriTrak-enabled workplace and how long they have been there.[84]

DigitalAngel is a pager sized GPS device that children and the elderly can wear, and in the event of an emergency, such as a fall or if signaled by the user, the device will alert emergency workers to the user's exact location. ADS hopes that in the future it will be able to incorporate DigitalAngel with VeriChip, allowing for GPS-assisted tracking of loved ones.[85]

On 13 April 2004, ADS announced that it had entered a memorandum of understanding with FN Herstal, manufacturers of both Browning as well as Smith and Wesson firearms, in which they plan to develop "Smart Guns." [86] The idea is that the firearm would only be functional when the owner, who has the corresponding VeriChip, was holding the weapon. There would be a VeriChip scanner located in the gun calibrated to fire only when it received the personally identifiable number from the owner's VeriChip.

Analysis Framework

The potential applications of the VeriChip technology results in many revealing and interesting human equivalents. When VeriChip is used to access healthcare information, the human equivalent would be someone who tells healthcare workers the patient's vital medical information and history. Under the guidelines of HIPAA, only specific, predetermined people would have access to the patient's medical records. Addressing this concern, ADS already makes sure that only registered users can access its GVS registry.

It is disconcerting that one's personally identifiable VeriChip number is broadcasted. The human equivalent of this would be someone shouting out the patient's driver's license number. Though a driver's license number by itself means nothing, one could process that number to extract information about the owner. Likewise, though knowing the VeriChip's ID number means nothing in itself, in the future there may be plenty of databases though which one may gather information about a person simply by running a query of the number. There are no easy opt-out methods for a VeriChip implantee (e.g. the user cannot insert and take out the device according to his wishes), so the task of protecting of a person's information rests with VeriChip, and therefore ADS as well. Though the chip is not yet a pervasive method used to access healthcare information in emergency situations, there is growing interest in the product.

---

[84] ADS website.
[85] Paul Eng. "Implant Chip, Track People." *ABC News*, 25 February 2004. http://abcnews.go.com/Technology/story?id=98077&page=1
[86] ADS Press Release. http://adsx.com/news/2004/041304.html

Considering ADS is launching its “Get Chipped” campaign and instituting mobile implanting centers, there is certainly a possibility that in a few years VeriChips will be very common. Since the VeriChip Health Information Microtransponder System is still in its beginning stages, ADS should address the system’s privacy issues before the system becomes pervasive. Just as there exists stringent protections against access to driver’s license and social security databases, including protections for the numbers themselves. There should be strong measures implemented to protect VeriChip information.

When the VeriChip is used as a tracking device, such as in VeriKid or a future VeriTrak or DigitalAngel system, the human equivalent would be someone standing in a public place taking note of every person that walks through the area without necessarily ever alerting passers-by of his intentions and then keeping that record for an indefinite amount of time. Though the act of keeping these records itself should not be a cause for alarm, what is done with these records is. The person could take the records and sell the information to marketers, or use the information in other malicious ways. There could be cases where “tracking” would easily mean either “stalking” by predators or “monitoring” by the government. One could easily imagine civil liberties groups condoning the situation, raising concerns about privacy rights. Similarly, if Solusat were to log every person that walks through its public scanners in search of a VeriKid, it would have a large database tracking the movements of many VeriChip users. What is of great concern is what happens to that data and who has access to it. If the database is not encrypted, then anyone could easily access the movements of innocent VeriChip users without their knowledge or consent; even if it was not encrypted, there is still a chance that these records could be used for purposes far beyond simply trying to find a VeriKid. Therefore considering that these systems have not been implemented yet, we strongly believe that ADS and Solusat should design the system so that no records are kept other than the movements of the VeriKid in question or the DigitalAngel user, and that all records are strongly encrypted.

All VeriChip systems eventually lead to the same purpose: identification of its owner. Under this framework’s identification-potential spectrum, all VeriChip systems are near the active end of the spectrum; they actively identify the user through processing of the data. Each of these systems collects, stores, and processes the information to identify the owner, regardless of whether it is for medical purposes or for buying drinks at the Baja Beach Club. What PAPA accomplishes is that it limits the abusive identification, beyond the services on which the user agreed, of the system and unwarranted tracking of individuals by regulating the distribution of the stored information, thereby preventing VeriChip’s further movement into the active end of the spectrum. By limiting distribution, it prevents the information from being used for purposes other than those clearly outlined. For example, a VeriMed user could not be tracked by a public VeriKid system because he did not agree to that service, and his employer could not use the private VeriTrak system to track him in the office without his knowledge; he wants the VeriChip to be used for only medical purposes, and for that reason he cannot be tracked and monitored without his consent. It may even potentially help push the system toward the passive side by regulating under what circumstance the information can be stored. By doing so, PAPA would help in

protecting the public anonymity of VeriChip users as well their records. It would assure the public that the VeriChip was not used for purposes other than those designated.

	VeriChip on the Analysis Framework
Human Functional Equivalent	• Medical: having someone ready to give medical information in case of emergency • Tracking: having someone keeping record of every person going through a public place at any given time
Consent: Opt-in or Opt-out	Voluntary surgery, so can choose not to get implanted Once implanted, no opt-out policies currently if future policies change
Pervasiveness	VeriKid would place sensors in public places; become quite pervasive Medical is not pervasive yet; potential to become pervasive with volumes of sales; mixing of databases (i.e. mixing VeriKid tracker with medical ID) could mean those who signed up for simply having medical records in emergency could also be tracked and monitored without consent anywhere in public places
Personally Identifiable	At present, near active end of the spectrum. Purpose *is* to personally identify owner.

Table 2: Summary of Application of Analysis Framework in evaluating anonymity and privacy concerns in VeriChip.

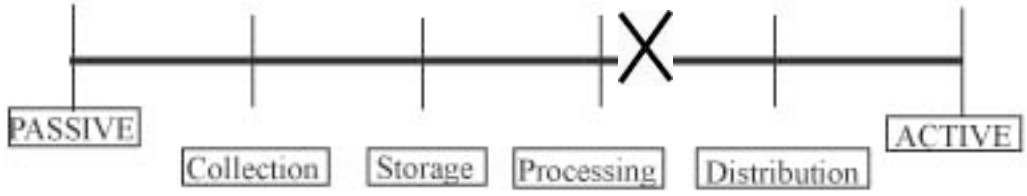

Figure 2: VeriChip is best placed at Processing on the Identification Potential Spectrum. All VeriChip systems collect, store, and process the 16-charater personally identifiable number associated with each chip to identify its owner. No legislation prevents it from becoming further active by entering the Distribution zone.

Concerns

There are several concerns raised by VeriChip. The first two main security measures that ADS provides are that only those healthcare providers registered with ADS may access the data, and the data between the scanner and ADS's database is sent via a secured internet connection. However, this raises a few concerns. The first concern is that the data sent from the VeriChip to the proprietary reader is not encrypted. This is a problem because that means anyone with an RF reader will be able to scan a subscriber's VeriChip without the owner ever knowing his information was scanned. While the only information the scanner would gather is the user's personally identifiable number, no other information about the owner would be available from the scan itself without access to the GVS. However, the person

scanning the VeriChip would be able to link each person scanned by taking a picture, video clip, or simply remembering the person's name with the owner's personally identifiable number. Afterwards, the scanning party could create a separate database and then either sell it to marketers or use it for malicious purposes, all without ever asking the user's permission or even alerting him that he was being scanned. The same person could set up his own network of hidden scanners in public places and, having linked certain people with their VeriChip number, would be able to track individuals. Jane has ID "12DF3." Joe sets up simple, cheap scanners around those places Jane regularly visits, and every time "12DF3" passes through a detector, he knows where Jane is and can go there to follow her.

Another concern that arises is who has access to the databases, both the GVS as well as any third party databases created for private use, such as for the Baja Beach Club's VIPs. Soon, there will be several more databases incorporating all types of information about VeriChip users in the hopes of providing more convenience. The British civil liberties group, Liberty, states that

> the arrival of such tracking chips needs to be matched by a tougher legal framework to protect people's privacy . . . and that more questions need to be asked about how the information gathered will be used and protected."[87]

ADS states that they are concerned about customer privacy and that they encrypt the data in the GVS. However, they do not mention who within the company can see the data; arguably, the more people have access, the less secure it is. Along with the concern of who had access to records is another concern regarding how long records are kept. Particularly concerning in the VeriKid situation, where sensors are placed in public places scanning for VeriChips, the system could easily be abused, either intentionally or unintentionally, such that it records every VeriChip user that walks through the scanner, regardless of whether it was the missing VeriKid, paving the way for human LoJack.

Consider an example. A VeriChip user named Joe walks through a public scanner on his way to the movie theater, unaware that there is a search for a VeriKid in the same area and so all nearby VeriChips are being scanned. Five years later, Joe's movement records from the VeriKid system are subpoenaed to show exactly where he was at that time, as his wife is trying to prove his infidelity in divorce hearings. Joe never agreed to being subjected to tracking in public places. He simply had a VeriChip implanted so that his medical records would be handy in case of an emergency. Now, the very device that was supposed to save his life is being used to track his movements the same way scientists track migration patterns. He did not consent to these uses and he cannot opt-out of a surgically-implanted device. Compare this example to the possibility of Joe choosing not to use a credit card that adversely changes its privacy policies. Joe never had the opportunity to opt out of the tracking service. Meanwhile, a hacker, impervious to Joe's current predicament, is able to hack into the weakly encrypted VeriKid database and download all the data to sell online. The intent of VeriChip to improve Joe's life has now dealt three strikes against him. This scenario demonstrates the lack of policy as well as the disregard of security led to the

[87] Sean Coughlan. "Security Under the Skin." *BBC News World Edition*, 15 October 2004.

loss of anonymity and of sensitive records.

Recommendations

So what should be done to prevent this type of scenario? First, ADS must clearly establish that it only records information that the user has allowed the company to record, it will be used only for the purpose clearly defined, and it stores the information for only an amount of time with which the user agrees, so that if Bob does not want any movement records kept and only wants the chip for use in medical emergency scenarios, ADS should abide by his terms. Second, the VeriKid system should not record all VeriChip movements through its scanners. It should be an instantaneous system that, only when it detects the VeriKid, it records the VeriKid's location and time, but it never records any other VeriChip user. This system of using public sensors to scan chip users has the potential to be abused far too easily by recording the movements of all VeriChip users, so ADS and Solusat should make it policy that this does not occur. Third, all databases regarding a VeriChip, regardless if it is the GVS or the Baja Beach Club roster, must be encrypted. Since ADS is the manufacturer of the product, it should mandate that all third-party and value-added resellers abide by these rules or risk losing their VeriChip licensing rights. Again, this system could be abused far too easily, especially if the databases are not encrypted. If VeriChip does not insist that its users are protected, then the government must act in the interest of the chip users. Just as credit card records are secured under the Fair Credit Reporting Act, among several other acts, and medical records are protected under Health Insurance Portability and Accountability Act, so too must VeriChip records be protected. Finally, there must be some level of protection that protects the VeriChip user from government abuse. If there is no legislation outlining specifically what the government can and cannot access without a court order, then there is a possibility of a civil liberties crisis in which all VeriChip users can be tracked and monitored in public areas by a Big Brother-like government. The legislation will clearly state under what circumstances the government may request VeriChip records. Later in this paper we will show how PAPA successfully addresses all of the aforementioned concerns.

Retail RFID Use

On 15 November, 2004, the Food and Drug Administration announced that several pharmaceutical companies would begin putting RFID tags under the labels of the larger, bulk bottles that are sent from the manufacturer to the pharmacies to combat counterfeiting and fraud[88]. Currently, Pfizer will implement the RFID system on Viagra while Purdue Pharma will tag its bottles of OxyContin, both of which are two of their most counterfeited and abused drugs. The hope is, by outfitting drug packages with RFID, the pharmaceutical companies will be able to trace the drug's route from manufacturing to the pharmacy where it is dispensed.

---

http://news.bbc.co.uk/2/hi/uk_news/magazine/3742684.stm

[88] Gardiner Harris. "Tiny Antennas To Keep Tabs on US Drugs." *New York Times*, 15 November 2004. http://www.nytimes.com/2004/11/15/health/15drug.html

But pharmaceutical companies are not the only ones to incorporate RFID into the goods they sell to consumers. Retail giants Wal-Mart and Sears have announced that they will soon use RFID to streamline inventory tracking. Gillette and Wal-Mart had teamed together to design “smart-shelves” that know how much of a product is available on the shelves and can order more automatically if supplies dwindle[89], but eventually Wal-Mart pulled out of the project after listening to privacy advocates.[90]

Concerns

Using RFID on wholesale prescription bottles holds promise in reducing counterfeiting by giving companies the ability to scan the bottles at every point of its route to the pharmacist. Nevertheless some privacy-rights groups raise concerns about what might happen if the same technology is incorporated into the smaller consumer prescription bottles.[91] They feel that by incorporating tags into prescription bottles, it allows outsiders to scan passers-by and record what medications they may have on their person. In fact, the concern is much broader and can incorporate other retail RFID uses, such as those by Wal-Mart and Sears. But the main concern is that there is no legislation or industrial regulations stipulating important facts, such as what purpose the RFID tag serves, how long the tag can remain on the merchandise, who has access to its electronic records, and how to protect the consumers who buy the products from being unlawfully tracked. Though Wal-Mart has assured privacy activists that RFID will only be used in its warehouses, in the near future many other retailers may begin putting RFID tags on the products they sell. As ubiquitous as RFID use is becoming without any legislation limiting its misuse, there could be situations where the RFID on consumer products might be used for purposes beyond simply inventory tracking.

Consider a situation where a person is able to link another individual's identifiable information to his RF signal using a network of ubiquitous sensors stationed in public areas, similar to VeriKid systems. Once linked, that signature can be tracked throughout the network of hidden public RFID scanners. So the RFID tags in Bob’s shoes, shirt, watch, sunglasses, underwear, socks, and jeans can be linked to him, but the database could be thorough enough so that, even if Bob simply wore the same socks on a day different from the day he was entered into the database, he could be easily tracked.

The concern is that the widespread use of RFID may allow corporations to track customer movements. They could compile the data and find what the consumer buys and where the product, and therefore by extension the consumer, travels. The compiled data could be used to create consumer profiles, which would include inferential assumptions about buying habits, interests, health, lifestyle, travels, and even income. These profiles could then be sold as dossiers on individuals to governments or to other companies. Though at present such scenarios are unlikely regarding the RFID tags in consumer

[89] "Gillette Pioneers Breakthrough Technology," *Yahoo Business Wire*, 6 January 2003. http://biz.yahoo.com/bw/030106/62365_1.html

[90] Alorie Gilbert & Richard Shim, "Wal-Mart Cancels 'Smart Shelf' Trial," *CNET News.com*, 9 July 2003. http://news.com.com/2100-1019_3-1023934.html?tag=fd_lede1_hed

merchandise, privacy advocates are concerned that measures to protect consumer privacy (such as how much information is collected, why it is collected, who has access) are stagnant while RFID technology and ubiquity is increasing.

In fact, under the Electronic Product Code (EPC) Global RFID standard, each individual RFID would have its own unique ID, unlike UPC barcodes, where the barcodes would differentiate the different products, not the individual instances of products. Under the EPC, the data would be stored in the Object Name Service (ONS), a centralized global database would store information on the RFID tag, and readers could connect to it via the internet and modify the tag's records throughout its life cycle.[92] EPCGlobal chose Verisign, Inc. in January 2004 to manage the ONS[93], a fact that has raised concerns among privacy advocates due to Verisign's poor electronic privacy record. Privacy advocates in 2003 criticized Verisign's SiteFinder, which, instead of responding with an error message, would direct mistyped email and web addresses in the company's .COM and .NET top-level domains to Verisign's own websites to promote its commercial services. By redirecting mistyped email addresses, it made it possible for Verisign to intercept and store private emails.[94] So privacy advocates concerned with RFID worry that Verisign may abuse its ONS for personal commercial gain as well.

Privacy groups are concerned about the fact that an RFID tag, once attached to merchandise, can be used for tracking purposes indefinitely. As such, they have suggested that consumers consider crushing the tags or punching holes through them to protect themselves. In response, the RFID industry has proposed several solutions to ease consumer tensions, including EPCGlobal who has offered a solution to "kill" tags at the point of sale by the merchant.[95] They have even hired the public relations firm of Fleishman-Hillard in order to help promote a more positive image of RFID.[96] Privacy advocates however do not believe that "tag killing" is effective, since it simply sends a "kill" command to the tag, which has been shown to be buggy and not to work always, and which could be brought back to use with the proper initialization command.[97] Until the industry can come up with an effective solution, the government must create legislation in the interest of consumer protection regarding RFID that deals with who has access to ONS, why product is tagged and to make sure its purpose does not go beyond that, and how to destroy the tag when sold to consumer.

---

[91] *NY Times* article.
[92] EPCglobal, "How the EPC Network Will Automate the Supply Chain," http://riccistreet.net/port80/charthouse/future/rfid.htm
[93] Paul Roberts. "VeriSign to Manage RFID 'Root' Server." *The Industry Standard*, 13 January 2004. http://www.thestandard.com/article.php?story=20040113174055565
[94] SecurityFocus. "Verisign's SiteFinder Finds Privacy Hullabaloo." *The Register*, 19 September 2003. http://www.theregister.co.uk/2003/09/19/verisigns_sitefinder_finds_privacy_hullabaloo/
[95] Junko Yoshida. "RFID Backlash Prompts 'Kill' Feature." *EE Times*. 28 April 2003.
[96] Jane Black. "Playing Tag With Shoppers' Anonymity." *Business Week*, 21 July 2003. http://www.businessweek.com/technology/content/jul2003/tc20030721_8408_tc073.htm
[97] Jo Best. "Zombie RFID Tags May Never Die." *ZDNet*. 18 May 2004.

Analysis Framework

The human-equivalent of RFID in retail use would having someone tracking every piece of merchandise from the point it is manufactured all the way through its sale to the consumer. A major concern is the tracking of same piece of merchandise and its owner for an indefinite amount of time after it was sold. Since the human-equivalent form would amount to stalking or illegal surveillance, similarly, there must be legislation forbidding such post-sale tracking using RFID tags.

Presently, the industry does not offer an effective opt-out procedure, where consumers will be able to have the RFID in their merchandise permanently "killed" at the time of sale, nor are there any opt-out options preventing post-sale tracking of "unkilled" RFID tags. RFID tags are becoming pervasive in merchandise tracking, yet current regulations and legislation are not keeping pace with the spread of the technology.

The retail application of this technology lies near the passive end of the identification-potential spectrum because its purpose identifies merchandise, not people. Yet there is far too much potential for this technology to be abused. By simply linking a person to an RFID-tagged product, its potential of being personally identifiable shoots into the active side of the spectrum, and if this happens, then the product effectively becomes dangerous to the consumer.

Just as there are State and Federal laws that protect consumers from purchasing dangerous products without knowledge of its dangers, so must there be laws that protect and prevent the misuse of RFID and any other future inventory tracking technologies. These laws must protect public anonymity and keep RFID and all inventory tracking technologies from hindering privacy. Consumers must be made aware that the product they are purchasing contains an RFID chip, and they must be given the option to have the tag destroyed permanently at no cost (consumers should not have to pay extra for their right to anonymity). Companies like Verisign will not be able to abuse the ONS to gain personal profit by compromising consumer privacy. Consumer information shall not be linked to the RFID tag database in any way, especially any information that would allow the tag to personally identify the owner. Post-sale, the RFID tag will no longer be tracked for any purpose whatsoever, thereby also preventing, by extension, the tracking of the merchandise's owner; its purpose has been served, and it must be destroyed if the consumer wishes. PAPA addresses all of these concerns in protecting public anonymity from both private and public entities.

	Retail RFID on the Analysis Framework
Human Functional Equivalent	Having someone track the merchandise throughout the supply chain. Laws prevent this person from tracking the merchandise – and by extension its owner – after the sale (stalking, privacy), so there must be such laws for tracking technologies, such as RFID.
Consent: Opt-in or Opt-out	Consumers at present do not have an opt-out procedure. There must be regulations mandating that tags are destroyed

	at point of sale.
Pervasiveness	RFID in retail is quickly being adopted, so potential to become highly pervasive soon.
Personally Identifiable	Near passive end of spectrum. Purpose is not to identify owner but to ID product. Can easily be shifted to active end if spectrum if personal information is linked to ONS database.

Table 3: Summary of Application of Analysis Framework in evaluating anonymity and privacy concerns in RFID in retail use.

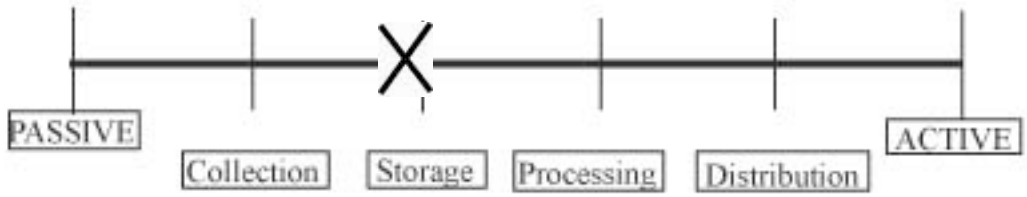

Figure 3: RFID in retail is best placed at Storage on the Identification Potential Spectrum. RFID tags at present are used to ID merchandise, not its owner. By adding personal information to the database, it could easily shift to the Active end of the spectrum, and there is no legislation preventing that.

Electronic Toll Collection

Electronic Toll Collection (ETC) systems are Intelligent Transportation Systems consisting of RFID tags and are used to pay highway tolls. Millions of drivers pass through toll booths daily, and most toll roads in America are equipped with some sort of ETC system that processes tolls electronically. Each system consists of an in-car transponder, which is a battery operated RFID unit affixed inside the car's windshield that operates in the 900-MHz band. As the car approaches the tollbooth, it either crosses a treadle (pressure strip on the road itself) or breaks a light beam, which in turn activates the transceiver antenna positioned above the road at the booth.[98] The transceiver activates the car's transponder unit and queries it for its associated account information, which the transponder broadcasts back. The transceiver's host computer identifies the information and, if the driver has a valid account, deducts the toll amount from that account. SIRIT and TransCore are the two main manufacturers of ETC systems

In the past few years, ETC systems have been used for many purposes that go beyond the realm of simple toll collection. For example in New York and New Jersey, drivers will be able to pay for their parking at JFK, Albany, and Newark Airports using their E-ZPass accounts[99], while drive-thru patrons at select McDonald's restaurants can pay for their meals as well. [100] In Houston, the city electronically maps traffic congestion by keeping track of how many TXPass transponders pass key points at any given time,

[98] Kevin Bonsor. "How E-ZPass Works." HowStuffWorks. http://auto.howstuffworks.com/e-zpass.htm
[99] E-ZPass Plus. Port Authority of New York and New Jersey. http://www.panynj.gov/ezpass.html
[100] "McDonald's Testing E-Payment System." *USA Today*, 29 May 2001. http://www.usatoday.com/tech/news/2001-05-29-mcdonalds-e-payments.htm

and then using that information they create a real-time map showing traffic flow.[101] An Illinois man used his wife's I-Pass records to prove his wife's infidelity during divorce hearings by showing which highway exits she would take and when.[102] These and other examples show how ETC systems and records are going beyond their preliminary use of simply paying tolls and how there is a need for legislation to protect consumers.

Non-toll uses of ETC

There are several instances where ETC systems have been used for purposes other than toll collection. In fact, there are several cases in which courts have ordered records released for civil and criminal cases. For example in 2003, the City of New York used the E-ZPass records from thirty of its narcotics agents to show that they had falsely claimed $45,000-$50,000 in overtime pay.[103] The records showed that the officers were never near those areas where they claimed to have been working during their claimed overtime hours. Another example involves the investigation around the death of Assistant Attorney General Jonathan Luna.[104] In 2003, Luna was founder murdered in Lancaster County, Pennsylvania while traveling there in his car from his home in Maryland. Luna was to have prosecuted a case the following day in Lancaster County, so why he went there was not of concern. However, after FBI agents subpoenaed his E-ZPass records from the Pennsylvania Turnpike, they found that they way he got there was questionable, as he did not follow the most direct path from Maryland. Rather, by mapping his route using his E-ZPass record, they saw that his path was rather erratic. Though Luna's murder remains unsolved, access to his E-ZPass records has proved to be invaluable for the FBI in their progress of finding his killers.

ETC Systems are beginning to be used to pay for non-toll services as well. As previously mentioned, New York and New Jersey have implemented E-ZPass Plus, which allows drivers to automatically pay for airport parking using their E-ZPass accounts.[105] In Orange County, California, McDonald's allows drivers to use their FasTrak accounts to pay for their meals in four of their restaurants and plan to expand the service to fifty more. They have also implemented a similar program in Suffolk County, New York. Merrill Lynch analyst Peter Oakes found that people generally spent more when paying with FasTrak, noting that "[w]hen it's already paid, people are less hesitant and focus less on price and more on food."[106] Other companies, including rival Burger King, are watching McDonald's success with the system and are

---

[101] Rebecca Bolin. "Tracking, Traffic, and Toll Transponders." *Yale LawMeme*, 7 September 2004. http://research.yale.edu/lawmeme/modules.php?name=News&file=article&sid=1606

[102] Debbie Howlett. "Motorists Can Keep On Rolling Soon." *USA Today*, 25 May 2004. http://www.usatoday.com/news/nation/2004-05-25-toll-system_x.htm

[103] Shaila Dewan. "30 Narcotics Officers are Shifted in Shake-up Linked to Overtime." *New York Times*, 17 November 2003. Section B, Page 3.

[104] Kelli Arena. "Slain Prosecutor Alone at ATM Before His Death." *CNN.com*, 10 December 2003. http://www.cnn.com/2003/LAW/12/09/prosecutor.slaying/index.html

[105] E-ZPass Plus. Port Authority of New York and New Jersey. http://www.panynj.gov/ezpass.html

[106] "McDonald's Testing E-Payment System." *USA Today*, 29 May 2001. http://www.usatoday.com/tech/news/2001-05-29-mcdonalds-e-payments.htm

considering adding their own “ETC-friendly” payment systems as well.[107]

In order to gauge how expensive ETC reader systems are, we contacted SIRIT Technologies, makers of California’s FasTrak system.[108] We were informed that an antenna and transceiver control card combination would cost over $6,500 and that we would need CalTrans authorization to purchase such a system. We were unable to build our own transceiver set, but engineers at Texas A&M created their own in order to develop a real time traffic map.[109] The system, called the Houston Real-Time Traffic Map, sets up TxPass readers along Houston’s busiest roads.[110] The transceivers read the TxPass transponders in all the passing cars and feed the information to a centralized computer. The computer then creates a real time estimate of traffic flow and congestion and posts the information online so that commuters can gauge the estimated travel time to their destination.

Concerns

There are several concerns that are raised by toll collection systems in their current state. The biggest concerns to ETC drivers are the following questions: How easily is access granted to ETC records by the courts? How secure are the records? Who has access to these records? In the legal cases mentioned previously, either a subpoena or a court order could grant access to people’s ETC records depending on the type of case, whether for a divorce hearing or a murder investigation. Privacy advocates have also warned that states in need of cash may consider selling records to marketers.[111] Because of concerns that states may release records in any frivolous case if presented with a subpoena, or that they may sell sensitive information to marketers, many have passed legislation outlining to whom a person’s ETC information can be released and under what conditions.[112]

In 2001, New York Governor George Pataki introduced and passed an E-ZPass privacy bill.[113] The bill limits access to E-ZPass records to only state and federal court orders. By passing this legislation, New York will be able to prevent access from subpoenas tied to city or county level cases such as divorce hearings, yet still allow access for more serious cases such as the case involving overpaid New York officers or the investigation of Jonathan Luna’s murder. Other states have adopted similar privacy policies for their use and access of ETC records. Pennsylvania states in its E-ZPass privacy policy that access to its customers’ records are strictly forbidden except “in connection with a criminal law

---

[107] Ibid.
[108] SIRIT Technologies. http://www.sirit.com
[109] "Technology Helps Commuters Avoid Congestion." Texas Transportation Institute: Return on Research. http://tti.tamu.edu/product/ror/congestion.pdf
[110] Houston Real Time Traffic Map. http://traffic.houstontranstar.org
[111] Garfinkel, Simson. Database Nation. Cambridge: O’Reilly, 2000.
[112] VDOT'S Smart Tag - Protecting Patron Privacy. Virginia Department of Transportation Privacy Policy. https://smart-tag.com/privacy.cfm
[113] Richard D'Errico. "Pataki Announces E-ZPass Privacy Bill." *Business Review*, 6 June 2001. http://www.bizjournals.com/albany/stories/2001/06/04/daily36.html

enforcement action."[114]

We contacted the Massachusetts Turnpike Authority and enquired into their FastLane privacy policies. We were told that, like other states, records are kept for as long as the account is active. Under Massachusetts General Laws regarding FastTrak, all the information would remain strictly confidential, and that records would "be used for enforcement purposes only with respect to toll collection regulations."[115] However, there are no auditing or oversight groups to make sure that many of these states follow these guidelines. As hard as states try to protect the privacy of their ETC consumers by passing legislation, they must also be accountable for the security of the actual databases. In 2001, a programmer in Pennsylvania found a security flaw in a northeastern state's E-ZPass database that allowed him to view countless records and let him "view names, addresses, account numbers and detailed logs noting every time a car breezed through a toll booth."[116]

The question of who has access to the database becomes even more prominent once we investigate cases where ETC systems are used for purposes other than toll collection. Consider the example of customers paying for their meals at McDonald's with their E-ZPass or FasTrak accounts. Here is a situation where the account information is transmitted from the car to the McDonald's, then McDonald's sends that information to the state so that the driver's account can be deducted, then the state credits the restaurant the cost of the meal. One sees here that a driver's information goes through several different databases and networks in order to pay for the meal, so this raises a few questions. First, how secure is the network? If the network is not encrypted, then the driver might as well flash his personal information in public; the transaction goes through far too many networks and computers to not be secured without putting the consumer at risk. Second, what information is gathered during the transaction? Does the McDonald's system record what was purchased and the link it to the E-ZPass account number? Third, is this information kept in the E-ZPass record as well? Namely, would it be possible, depending on the state and its privacy laws, to subpoena a person's ETC records and show not only where they traveled but also where they ate? Because the system is still so new, no information is available to answer these questions. Furthermore, there is no legislation limiting the use and access to these new third party databases (e.g. McDonald's, Houston Real Time Traffic Map).

Consider a scenario where Bob checks his city's real time traffic map online to see the congestion on the roads. The system has sensors that count E-ZPass transponders that pass by strategic points and calculates the traffic flow from that. For research purposes, the system also records these E-ZPass numbers. Bob passes these sensors daily to and from work. Usually on the way back, he stops by his

---

[114] E-ZPass Account Holder Privacy Statement. Pennsylvania Turnpike Commission. http://www.paturnpike.com/ezpass/privacy.htm

[115] Massachusetts G.L. c. 81A, Section 10. http://www.mass.gov/legis/laws/mgl/81a-10.htm

[116] Todd Wallack. "They Know where You've Been: Data Collected From FasTrak Drivers Raise Privacy Concerns." *San Francisco Chronicle*, 12 February 2001. http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2001/02/12/BU75523.DTL

favorite fast food restaurant and pays for his meal with his E-ZPass account. Whenever he flies to business trips, he parks his car in the airport and later pays for it automatically with E-ZPass Plus. It turns out that Bob has been missing work frequently lately, but he still claims overtime. Angered, his boss sues him and demands that Bob repay his salary and overtime payments. To prove their case, the boss's attorney subpoenas Bob's E-ZPass records. However, his state refuses access to anyone except for criminal cases or court orders from state or federal judges. The attorney knows that, while he cannot gain access to the state's E-ZPass database, there are plenty of third-party databases that Bob encounters daily, and because the state's legislation regarding E-ZPass privacy does not cover non-state databases, the attorney subpoena's the traffic map company, the fast-food restaurant, and the airport parking company. Because the signal from Bob's E-ZPass transponder is not encrypted, the attorney simply scans the device and gathers Bob's account number. He searches through all the databases for that number and creates a timeline and map showing Bob's movements and even his travel and eating habits, all by simply subpoenaing all the third parties who have access to Bob's E-ZPass daily. The example above shows that, while states are making progress in protecting their own ETC records, they must now consider a future where numerous third-party ETC databases will be linked together, and for whom the state's ETC legislation does not currently apply.

Analysis Framework

The human equivalent for electronic toll collection would simply be a tollbooth attendant who takes the driver's toll. However additionally, the attendant would also permanently write down where and the when the driver crossed through the toll plaza, as would all other toll attendants, and then they would all combine these records into one massive database. Because using ETC is voluntary, there is no opt-in or opt-out procedure that limits what information is gathered and for how long. The systems are fairly pervasive, as many states have adopted some for of ETC. As ETC systems incorporate more options beyond simply paying for tolls, these systems may become even more pervasive. On the Identification-Potential spectrum, ETCs fall under the active category. Their purpose is to identify the driver of the vehicle so that his account may be charged. The systems collect, store, and process the information to identify the driver. Many states haves adopted legislation that prohibits the distribution of this information by the state, so legislation does indeed exist to prevent the system from becoming further active at the hands of the government.

The human equivalent of the Houston Real Time Traffic Map system would be to have someone take note of how many cars go by certain strategic points at given times and then create a map showing the estimated traffic flow. The person might also keep a record of some sort of identifiable information about each car and create a database for research purposes. While there is nothing wrong or illegal about simply noting how many cars pass by, there is still the concern regarding what that information is used for and who has access to it. Is the person selling driving patterns based on license plate numbers to marketers? There is no opt-out system for this mapping, which is disturbing enough for song to bring

about products like the mCloak from mobileCloak.[117] The mCloak is a bag that blocks wireless signals from entering or exiting, and users can place their toll tags into the bags when they do not want their tags scanned. The traffic map system is pervasive only in Houston at the moment, as scanners are placed throughout the city in strategic, congestion-heavy areas. At present, a person cannot be personally identified by the system, so it falls in the passive end of the Identification-Potential Spectrum, but there is no legislation prevent the system from going towards the active end.

In the instances where ETC systems are used to pay for non-toll services, the human equivalent would be someone taking down a person's information and then running it by the state in order to have money withdrawn from the driver's account and placed in the company's. Additionally, it would keep a record detailing each transaction for its own records, creating a sizeable database. Though the database alone is not a cause for concern, many would question who has access to the databases, what information was kept, how secure it was, and for how long it was being kept. These are optional services now, so there is no opt-in or opt-out. At present, the systems are not very pervasive as they are slowly being adopted. Nevertheless it has potential to become highly pervasive if, for example, all drive-thru fast-food restaurants and pay-parking lots offered this service. These systems would be categorized in the active end of the Identification-Potential spectrum, as the purpose is to identify the user, process his information, and receive a payment from his ETC account.

	Electronic Toll Collection on the Analysis Framework
Human Functional Equivalent	Having someone deduct money from the driver's prepaid account, keeping a permanent record of when and wear the charge occurred, and compiling all such information into a database.
Consent: Opt-in or Opt-out	Since ETC is voluntary, consumers at present do not have an opt-out procedure. Having a second, prepaid digital cash equivalent would give drivers the same convenience of ETC but with the anonymity of paying with cash.
Pervasiveness	ETC systems exist in many states, and they are being adopted for purposes other than for paying tolls. These systems are becoming increasingly pervasive.
Personally Identifiable	Near active end of spectrum. Purpose is to identify the driver so that payment can be deducted from the associated account.

Table 4: Summary of Application of Analysis Framework in evaluating anonymity and privacy concerns in electronic toll collection systems.

[117] mobileCloak website. http://www.mobilecloak.com/mobilecloak/index.html

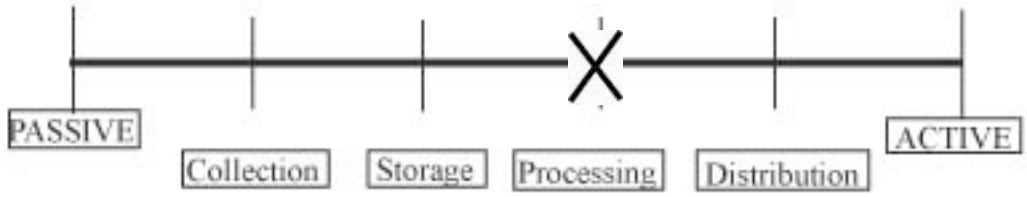

Figure 4: Electronic toll collection is best placed at Processing on the Identification Potential Spectrum. The systems are designed to identify the driver and having payment withdrawn from his account. Current legislations in many states prevents states from distributing the data, but there is no legislation preventing third-party databases from doing so.

Recommendations

We suggest pre-paid ETC transponders to protect consumers and individuals at the hands of RFID technology. Electronic Toll Collection systems should include an opt-out policy. Though the service is voluntary, we believe that users should be able to take part in the same convenience that systems like E-ZPass offers, such as driving through a toll booth without needing to stop, while also not being concerned with privacy issues. Would there be a market for such a prepaid E-ZPass? We believe so, as the mCloak bag, among other similar products, shows that there is indeed a market for anonymous ETC systems. We believe that, since ETC systems are solidly in place in several states, it would be unreasonable to demand a complete overhaul of all such systems to make them anonymous. Instead, we suggest that the government should encourage private entities (such as SIRIT and TransCore) to develop prepaid, anonymous ETC systems that could be bought and sold retail, much like prepaid phone cards or cellular phones. The prepaid anonymous systems will not be meant to replace the current ETC methods, as there are many who still wish to see their records monthly, as well the fact that it would not be cost effective or feasible to completely redo all the ETC systems in all states. Rather, we believe that it could be a secondary option for those who wish not to be tracked. Toll booths had an inherent anonymity when people paid with cash and continued on their path. However once ETC systems were created that logged all transactions, this sense of privacy quickly eroded away. While people concerned about anonymity can still pay with cash, they will not be granted to same functionality to take part in the convenience and speed that ETC systems provide. What would having a retail, prepaid ETC system solve? It would follow the principles of Digital Cash, where electronic transactions could occur with the same anonymity of cash and without the paper trail indicative of electronic commerce.[118] A user could purchase a prepaid transponder retail and then use it to pay for tolls, food, parking, or other ETC-dependent systems that may arise, all without ever having being personally linked to that ETC account, effectively acting as an opt-out to having one's movements tracked and stored. Essentially, this would recreate the same sense of anonymity that is inherent to paying tolls with cash but with the added convenience of using an ETC system.

[118] "Electronic Money." Wikipedia. http://en.wikipedia.org/wiki/Digital_cash

Conclusion

RFID systems show great promise for industries in helping to track, monitor, and identify inventory, merchandise, and people. However, these case studies demonstrate the potential for abuse without strong legislation protecting consumer privacy. Regulations on the tracking, monitoring, or identification of people should include provisions for searches violating the purpose for which the tag was originally designed and the user knowingly consented. For example, neither the government nor any private entity could track a VeriChip user without his consent or knowledge by using a VeriKid network of public sensors. In the case of RFID in retail, the RFID chip was implanted in merchandise for inventory tracking in the supply chain; a person should not be tracked using the RFID embedded in his purchases, and he should be able to opt-out by having the tag removed at the point of sale. Regarding electronic toll collection systems, third parties should not be able to create and distribute databases based on ETC users' movements without the permission of the users.

In general, people must be notified information about them is being collected using their associated RFID and if they are being tracked using RFID devices; told for what purpose he is being tracked, who has access to the records, and how long his records are kept; and be given a chance to opt-out. Records should not be processed and stored for a time longer than that which is required to serve its purpose unless the user specifies otherwise, such as indefinitely storing the records of an ETC transaction at the local McDonald's. In cases where it is necessary to collect and store RFID transactions, there should not be any "overprocessing," or processing the data in such a way that it goes beyond the information that is required for the transaction to occur. For example, currently during an electronic toll transaction, the time, date, location, and toll charge is recorded and stored with the associated account. There is no reason to overprocess the information about the person such as creating a second database that links travel patterns with shopping patterns as recorded with retail RFIDs or walking patterns as recorded by VeriChips, to effectively create a dossier about the person simply from RFID transactions. This also brings to light the fact that records should not be distributed beyond what is necessary for the transaction to occur, like above where there is no need to distribute all the different RFID information about a person to create a behavioral profile.

As prices for RFID sensor technology drops, we believe that companies and government will increasingly adopt the technology to streamline many tracking, monitoring, and identifying purposes. But the potential for these sensors to infringe on one's individual privacy should be a primary concern in its deployment. Just as there are measures to protect bank and medical records, so should there be strong legislation to protect against RFID abuse.

Biometrics

Biometrics is defined as the "automatic identification of identity verification of living persons using their

enduring physical or behavioral characteristics."[119] Though the field of biometrics is often considered an emerging or new technology, biometric devices have been in use for many years. In January 2000, there were already over 20,000 computer rooms, vaults, labs and other areas using biometric devices to control access.[120] Some commonly known biometric identifiers are fingerprints, facial recognition systems and retinal scans. As a growing surveillance method, it is crucial to analyze biometrics under our framework to demonstrate the growing trend in active surveillance methods.

Types of Biometrics

Fingerprints are one of most commonly used and known biometric identifiers. In the United States, the Automated Fingerprint Identification Systems is used by law enforcement for both forensics and criminal investigations.[121] While fingerprints have great invariability because they are difficult to modify or forge, fingerprints are not robust and can easily be damaged with chemicals.[122] In a study done by the DMV, only eight percent of the customers considered fingerprint identification invasive. In addition, since fingerprint identification systems are so common, there has been more testing done of these systems. The National Institute of Standards and Technology did a study of thirty-four commercially available fingerprint identification systems and tested over 48,000 prints in both large and small-scale application settings and with different fingerprint combinations. The NIST found that best system was 98.6% accurate for single fingers, 99.6% accurate for two fingers and 99.9% with four or more fingers.[123]

Retinal and iris scans are also becoming more common biometric identifiers. IrisScan, a maker of iris identification systems, has a machine that is capable of allowing video images of eyes to be taken from up to three feet away, illuminating the iris with infra-red light and memorizing the pattern. Iris recognition systems are capable of seeing through both glasses and contacts and can identify over 250 features. Iridian Technologies, the leading iris identification system company, claims that irises are the most accurate and invariable of all the possible biometrics.[124] In 2001, the United Kingdom's National Physical Laboratory tested one of the most common algorithms used in iris identification systems and found that with a sample of over two million people, there were no false matches.[125] Retinal scanners, on the other hand, require a user to look into a view-piece and focus on a visible target while the retina, a thin film of nerve endings inside the eyeball, is being scanned. While these systems have been commercially available since 1985, they are not as commonly used as fingerprint identification.

---

[119] Anonymous. "Biometrics,"<http://www.eff.org/Privacy/Surveillance/biometrics/>
[120] Erik Bowman. "Everything You Need to Know About Biometrics," (Identix Corp., January 2000), p. 1
[121]Bowman, p. 4
[122] Anonymous. "Biometrics," <http://www.eff.org/Privacy/Surveillance/biometrics/>
[123] Brian Robinson. "NIST Puts Fingerprints To The Test," July 19, 2004, Federal Computer Week, <http://www.fcw.com/fcw/articles/2004/0719/tec-fingerprint-07-19-04.asp>
[124] Anonymous. "Biometrics," <http://www.eff.org/Privacy/Surveillance/biometrics/>
[125] Tracy Staedter. "Iris Identification: How The Technology Behind Biometric Security Works," March 2003, MIT Technology Review, <http://www.technologyreview.com/articles/03/03/visualize0303.asp?p=1>

Vocal identification is another form of biometric identification used because of its ability to allow identification remotely using infrastructure that is already in place. However, vocal identification does not have a high accuracy rate and is extremely vulnerable to identity theft by tapping or bugging lines to capture the vocal identification. In addition, vocal identification systems are extremely subject to many variables such as discriminating the voice from background noise, identifying the voice under stress such as illness, exhaustion and aging.

One of the most controversial biometric identifiers is facial recognition, which identifies people based on their facial geometry. Facial geometry is based on taking a known reference point and measuring both distances and angles to other features. Another form of measurement is eigenface comparison that uses 150 facial abstractions and compares the captured video image to these abstract faces. While facial recognition is controversial since the 2001 Super Bowl, where law enforcement used facial recognition to scan the crowd without information the spectators, it has been used by the West Virginia Department of Motor Vehicles since 1998 to check for duplicate drivers' licenses.[126]

While there are many other types of biometric identifiers, such as signature, keystroke dynamics and hand geometry, only a few have been seriously considered and implemented into identification systems. Even those systems that have been implemented face the difficulties of accuracy, ease of use and ability to integrate into existing identification systems. It is difficult to look at biometric technologies as a whole because there are so many different biometric identifiers and because each identifier requires different equipment and provides a different set of information. For these reasons it is important to closely examine all the different possible biometric technologies under a unifying framework, while also considering the legal actions taken on biometric technologies.

Biometric technologies have been analyzed before under two different approaches. These frameworks examine each form of biometric technology individually and do not provide a way to abstract examine biometric technologies as merely a form of surveillance. One such approach is to analyze the technologies through characteristics inherent to the biometric systems. The second approach is to look at the technologies through the applications of the systems. We present these two approaches and then move to the analysis framework we have proposed to abstract biometric technologies.

Characterizing Biometrics

Since there are so many different types of biometric identifiers, it is crucial to analyze the different types of biometric identifiers under a framework that identifies different characteristics similar to all of the identifiers. These characteristics are robustness, distinctiveness, accessibility, acceptability and availability. Robustness is how repeatable a biometric characteristic is, whether or not it was subject to

[126] John D. Woodward, Jr. "Super Bowl Surveillance: Facing Up to Biometrics," 2001, RAND,

large changes. Fingerprints are not considered robust because they can be easily damaged with chemicals; however, facial recognition is considered to be robust. Distinctiveness is determined by whether or not the identifier is unique to the person or whether there are no large differences in pattern amongst a large population. Fingerprints, iris and retinal scans are considered extremely distinctive because they are uniquely identifying. However, hand geometry is not considered distinctive because there are only a limited number of patterns within the population and it is possible for many people to have the same identifier. Accessibility is considered to be whether the biometric identifier is easily presented to a sensor. Facial recognition is one example of a biometric identifier that is easily accessible. However, retinal scans that require a user to focus on an object within are not considered accessible because it takes more effort and is a more noticeable action. Acceptability is whether the user perceives the biometric as non-invasive. Even though facial recognition is easily accessible, it is considered invasive because a user lacks disclosure and the knowledge that such a censor is in place. Lastly, there is availability, which determines whether a user can present alternative forms of identification; for example, fingerprinting has high availability because there are ten possible fingerprints that could be used for identification. These characteristics can be summarized in a table that demonstrates whether each different biometric identifier fits into the characteristic:

Biometric Identifier	Robustness	Distinctiveness	Accessibility	Acceptability	Availability
Fingerprints	No	Yes	Yes	Yes	Yes
Iris/Retinal	Yes	Yes	No	Yes	No
Hand Geometry	Yes	No	Yes	Yes	No
Facial Recognition	Yes	Yes	Yes	Yes/No	No
Voice Recognition	No	No	Yes	Yes	No

Table 5: Characterization of Biometrics.

From this chart, we can see that fingerprints, iris/retinal recognition and facial recognition are the most feasible biometric options currently available because of each of these technologies is fairly acceptable to the population and easily understood and available.

Characterizing Applications

Then it is also possible to characterize the different applications of these technologies through a framework analysis. Each application can be characterized by examining the following characteristics: cooperative v. non-cooperative, overt v. covert, habituated v. non-habituated, attended v. non-attended, standard v. non-standard environment, public v. private, and open v. closed. It is important to look at this

---

<http://www.rand.org/publications/IP/IP209/IP209.pdf>, p.4

framework because it demonstrates that it is difficult to characterize biometric technologies through applications, which further shows the need for a system-based framework, such as ours.

Cooperative v. non-cooperative deals with the behavior of the user. If the user must voluntary cooperate in order to give the biometric information, that the system is considered to be cooperative. Biometric credit cards are considered cooperative because they require the user to voluntarily sign up for that particular credit card. However, facial recognition systems can be both cooperative and non-cooperative. While the facial recognition systems involved in biometric passports is cooperative because it requires voluntary agreeing and registering for a passport. At least within the United States, travel is not considered a right by the ruling in the case Gilmore v Ashcroft, which ruled the right to travel is not covered in the Constitution.[127] However, facial recognition such as that used at the Super Bowl in 2001 is non-cooperative because it involuntarily uses facial recognition systems on people who are unaware of such surveillance.

Overt v. covert is the characteristic that demonstrates whether a user is aware of such biometric sampling and identification. As in the example of facial recognition, it can be both an overt and covert sampling. In addition, iris scans can be covert as well, which is demonstrated in both London's Heathrow airport and Amsterdam's airport, both of which use iris recognition systems without notification in order to scan for known criminals and terrorists.[128]

Habituated v. non-habituated is a characteristic that demonstrates whether the system expects a certain level of experience from the user. Most systems are designed with both first-time users and experienced users in mind, particularly any systems designed to be overt by the government must be prepared to handle both experienced and inexperienced users.

Attended v. non-attended describes whether a system must be supervised while in use. For example, biometric passports require supervision while the biometric identification is initially being taken, though further verification will not require supervision.

Standard v. Non-standard environment, which describes how controlled the conditions are for operation. If conditions are extremely controlled, such as access to a restricted area, then it is considered a non-standard environment. Non-standard environments make sense for access requirements since restricting access requires control; however, in many cases, such as for security purposes, it is not good to have a controlled environment because it will lead to behavioral changes that will lessen the effect of the security policies. An example of a controlled environment would be an airport that has controlled access to many

[127] U.S. District Court for the Northern District of California. "Gilmore v. Ashcroft," No. C 02-3444 SI. <http://0-web.lexis-nexis.com.luna.wellesley.edu/universe/document?_m=b86a410217033450956a0955bd4a8344&_docnum=2&wchp=dGLbVzb-zSkVb&_md5=af003ba250f11fa8668b1c9ae64e7146>

parts; however, an example of an uncontrolled environment would be a park, where access to the park is not controlled or regulated.

Public v. private deals with whether the users will be customers or the general public or only a select few. In most cases where the system is being used for identification purposes, the systems will be public in order to scan the crowd. The same is true if the purpose is security, because it would not be worthwhile to only scan a limited number of people to ascertain if they were security risks. Lastly, it is important to decide whether the system is open or closed. An open system is one that is required to share the biometric information with other systems. Looking at these characteristics, it is possible to examine biometric systems through this framework, though it is important to examine them through the purpose of the systems rather than through the individual technologies:

Purpose	Cooperative	Overt	Habituated	Attended	Standard	Public	Open
Tracking	No	No	No	Yes/No	Yes	Yes	Yes/No
Identification	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes	Yes/No
Access	Yes	Yes	Yes	Yes/No	No	No	No

Table 6: Characterization of Applications of Biometrics.

From this chart, there is no clear-cut answer to most of the characteristics. However, it does demonstrate the vast difference in the requirements for the different purposes of the systems. From the inadequacies of this framework stem the reasons for our more abstract framework that allows us to apply it to a variety of technologies.

Analysis Framework

The framework our group has prepared looks closely at the following aspects of a surveillance system: human-equivalent, opt in/out, pervasiveness of the system, and identification.

If you consider what these technologies are replacing, it is clear that most of these jobs are those of security guards who would give access to restricted areas and provide responsibility for the identity of users. Therefore, biometric surveillance is legal in most cases, as are security guards and other human-functional equivalent positions.

An opt-in or opt-out scheme must be designed into the system. An example of an opt-in biometric system is the biometric passports, which require signing up and voluntarily giving a biometric identity. On the other hand, systems such as the facial recognition used at the Super Bowl are neither opt-in nor opt-out since they do not provide any choice to the user, but capture the biometric identifiers without permission. Therefore, biometric technology offers the option of opt-in/opt-out, but does not require such an option to

[128] Staedter.

be available.

Biometric technologies are not yet the most pervasive surveillance systems in place. However, biometric technology is becoming much more pervasive as both governments, and the private sector become further enthralled with the security and identification options that this growing industry offers and with the technology becoming easier and cheaper to manufacture, it becomes a more attractive alternative. The International Biometric Group based in New York City believes that the biometric industry will grow to $4.6 billion revenue by 2008.[129]

Identification is inherent in biometric technologies because they are designed to be so individuating and identifying. After examining the following chart, we classified biometric technologies as an active form of surveillance because, though legal through our comparison to human functional equivalents and often accompanied by an opt-in/opt-out policy, the growing pervasiveness and inherent personally identifiable-ness of the biometric technology demonstrates that it is an active form of surveillance.

Characteristics	Biometrics
Human Functional Equivalent	Yes
Consent: Opt-in or Opt-out	Dependent
Pervasiveness	Yes
Personally Identifiable	Yes

Table 7: Summary of Application of Analysis Framework in evaluating anonymity and privacy concerns in Biometrics.

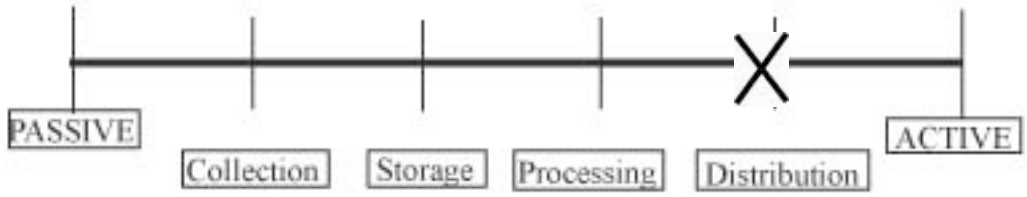

Figure 5: Biometrics is best placed in the active end of the Identification Potential Spectrum.

Within the examination of whether biometric surveillance systems are personally identifiable we also take a close look at the methods of collection, storage, processing and distribution. We also pictured these methods along an identification potential spectrum, such that collection is the most passive option of surveillance that gets progressively more active until distribution.

With biometric technologies, there is not just one instance of collection; there are always multiple

[129] Elaine Shannon. "Big Brother Inc.," 29 March 2004, Time Magazine,

instances. This is because it is necessary to make an initial capture of biometric information that is associated with a person and all further captures are compared against this initial capture. This means that the initial capture of the biometric information is crucial because it is deemed "true" and used as reference for all further inactions with the biometric system. This is problematic because it means that there must be multiple instances recording the time, date and location of a person's presence and gives criminals more instances to steal the information.

Storage refers to the databases and cards that the information is stored in. With biometric technologies, the security of databases and the information within is crucial because biometric information can be so uniquely identifying. Distribution and transmission between devices is also crucial with biometric technology because the transmissions must be secure enough that the information will not be stolen during the transmission, which must occur since the original captures are not stored with each individual sensor.

For biometric technologies, processing the information is most commonly used to match the current information with the "true" information stored in the database. However, biometric information can also reveal things other than just the intended identification. For example, iris scanning can also reveal medical disorders such as diabetes. In this case, the biometric identifiers could be provide more information than the system intended them to and could be over-processed in order to mine further information from the identifiers. In addition, processing must also be able to differentiate the biometric identifier from any other possible data that was received, which is called feature extraction. One of the reasons that vocal recognition cannot be implemented with a high accuracy rate yet is because it can be difficult to decipher what the identifier is and what the background noise is. The data that is being processed must also be checked for accuracy. For example, fingerprints are easily smudged while being taken or the wrong part of the finger, such as the tip, has been used instead of the actually fingerprint. If the database is large enough, then if might even be simpler to use pattern classification as well, which groups general patterns together so that the sample will only be tested against groups with the same features. For example, an iris scan sample of a person with blue eyes could only be tested against the group in the database with blue eyes, shortening the testing process.

Distribution with biometric technologies is also crucial to the protection of privacy and anonymity and warrants watching because it could allow the information that had been gathered to be used for other purposes. For example, if the biometric identification systems combined their information then it would be easy to convert all the points where a person's identification was required in order to track them. Our framework analysis demonstrates that biometric technologies are much closer to the active side of the spectrum rather than the passive side of the spectrum. Since biometric technology requires processing, it must be beyond the processing point; however, since not all biometric technology requires distribution, it

---

<http://www.time.com/time/insidebiz/article/0,9171,1101040405-605473,00.html>

lies between processing and distribution.

This framework allows us to examine many different types of technologies, and also to look at biometrics as a whole, rather than split up by the individual technologies. Another important part of our framework is the identification potential spectrum. In order to protect a person's privacy and anonymity in public spaces it is important that these technologies be as passive as possible while acknowledging that for security purposes it might be necessary to have some more active sensors.

Biometric technologies are extremely active technologies. It is necessary for the data that a biometric sensor receives to be processed in order to be used and has the capability to be easily over-processed and distributed. In addition, there is no regulation that prevents the government or the private sector from storing the information they collect for as long as they like or from being mined for further personal and identifying information. While the legislature has, in the past, required that storage facilities for biometric information be secure, there is nothing to prevent the theft of the information during transmission or from widespread distribution.

Current Legislation

Biometric technologies have been implied in legislation since the mid-1990s. In 1995, there was the Personal Responsibility and Work Opportunity Act, which required and implementation of an electronic benefits transfer program "using the most recent technology available […] which may include personal identification numbers, photographic identification […] and other measures".[130] While this does not directly refer to biometric technology, there is no question that this act implies the responsibility of the federal government to use the most recent and most accurate identification technology available with no restrictions on what type of information is used for identification, how long this information is stored and whether the information can be shared. The following year, in 1996, there was the Immigration Control and Financial Responsibility Act, which required the President to "develop and recommend […] a plan for the establishment of a data system or alternative system […] to verify eligibility for employment […] and immigration status".[131] While this act, too, does not directly refer to biometric technology, it does require the government to create a database system that seems similar to one that a biometric identification system would require.

---

[130] "Personal Responsibility and Work Opportunity Act of 1996," CIS-NO: 96-H271-70, CIS-DATE: December, 1996, SOURCE: Committee on Commerce. House, DOC-TYPE: Hearing , DATE: June 11, 1996, LENGTH: iii+96 p., SUDOC: Y4.C73/8:104-102, CIS/Index, < http://0-web.lexis-nexis.com.luna.wellesley.edu/congcomp/document?_m=c99c5f266641dd42e33ff64fdfcef566&_docnum=2&wchp=dGLbVzb-zSkSA&_md5=620553d938990f553a3fc2cd9ae426af>

[131] "Immigration Control and Financial Responsibility Act of 1996," CIS-NO: 96-S523-3, CIS-DATE: April, 1996, SOURCE: Committee on the Judiciary. Senate, DOC-TYPE: Report, DOC-NO: S. Rpt. 104-249, DATE: Apr. 10, 1996, LENGTH: 146 p., SUDOC: Y1.1/5:104-249, CIS/Index, < http://0-web.lexis-nexis.com.luna.wellesley.edu/congcomp/document?_m=84f71f22ec8a491ba40fb00d07edf328&_docnum=1&wchp=dGLbVzb-zSkSA&_md5=3ad74e9d396651b6040e77a93cd95cfc>

In 1996 there was also the Illegal Immigration Reform and Immigrant Responsibility Act, one of the first pieces of legislation identifying biometric technology. This act required the Immigration and Naturalization Service (INS) to include "a biometric identifier that is machine readable" on border crossing cards.[132] Not only does this act require the use of biometric identifiers, but it also implies the use of a database as storage of the information and in order to process and read the border crossing cards. However, what is not required of the INS or the federal government is any discretion on the information collected or the use of the information after its initial collection and during subsequent collections.

The Truck and Bus Safety and Regulatory Reform Act of 1988 required all commercial drivers to carry identification with biometric information on them and created standards for this identification.[133] Though this act required the federal government to develop standards for biometric identification, none of the other federal acts mentioned thus far require the development of any standards and thereby the creation of an evaluating system and policy.

The State of California the Digital Signature Law in 1998 that dealt with the biometric identifier, digital signature, and created a four-part test with which to ensure the security and uniqueness of the digital signature. This test not only required that the signature be unique to the maker, but it must be capable of verification, under the sole control of the maker and any attempts to make an altercation will result in the invalidation of the digital signature. This law demonstrates that it is possible to enact a law that will not only allow biometric identifiers, but will protect the information and strengthen the genuineness of any digital signature that passes the four-part test outlined in the law.

In more recent legislation, there has been no concern for the safety of the information, but rather a stress on more surveillance in order to promote security. The USA-PATRIOT Act gives a greater freedom to law enforcement agencies that provides the government with "Enhanced Surveillance Procedures" by granting them further capabilities in the interception of wire, oral and electronic communications. In addition, the USA-PATRIOT Act also provided law enforcement agencies more freedom to share information in criminal investigations, allowing such disclosures in many situations such as

> "when the matters involved foreign intelligence or counterintelligence […] or foreign intelligence information […] to any Federal law enforcement […] in order to assist the official receiving that information".[134]

While this limits the information able to be shared to "foreign intelligence" or "foreign intelligence information", these terms are also extremely loosely defined. In the act, "foreign intelligence information" is defined as, "information, whether or not concerning a United States person, that relates to the ability of

---

[132] "Illegal Immigration Reform and Immigrant Responsibility Act of 1996"
[133] "Truck and Bus Safety and Regulatory Reform Act of 1988," as quoted in "Biometrics", <http://www.eff.org/Privacy/Surveillance/biometrics>
[134] "107th Congress. "PATRIOT Act". 26 Oct 2001. <http://news.findlaw.com/cnn/docs/terrorism/patriotact.pdf>

the United States to protect against – […] actual or potential attack, […] sabotage or international terrorism, […] or clandestine intelligence activities".[135] It also considers any information that deals with the national defense or the conduct of the foreign affairs of the United States.

This loose definition provides the ability of law enforcement officials to claim the need of all sorts of information for security or defense needs. In addition, the USA-PATRIOT Act also brings up the problems of visa integrity and security, requiring the federal government to, "develop and certify a technology standard that can be used to verify the identity of persons" applying for visa in order to conduct, "background checks, confirming identity, and ensuring that a person has not received a visa under a different name."[136] This act not only provides greater freedom to the law enforcement agencies in the collection and processing of the information gathered, but it pushes for a form of identification and technological standards to be developed to enforce this identification.

This push for a technological standard for identification is pursued in the Enhanced Border Security and Visa Entry Reform Act of 2002 that requires, "machine-readable, tamper-resistant visas and other travel and entry documents that use biometric identifiers" to be issued to all foreign visitors and residents by October 2004. While this act requires the use of biometric identifiers outright, it also requires some measure of security in order to ensure that these visas are "tamper-resistant". In addition, this act requires that the technology shall "utilize the technology standard established pursuant to section 403 (c) of the USA-PATRIOT Act".[137] What the act does not detail, however, is any limitation on the biometric information required in these visas or the safety of the information within the databases required to store the information.

This act, along with the USA-PATRIOT Act, has developed into the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program.[138] This program was initiated by Congress in 2002 and is planned to spend $10 billion over the next decade. This program was set up to enhance the security of the citizens and visitors, facilitate legitimate travel and trade, ensure the integrity of the immigration system and to protect the privacy of the visitors. This program requires two index fingerprints and a digital photograph from each visa applicant as their biometric identifiers. In addition, other countries are being required to place biometric identification into their passports, while the State Department is issuing all new passports with an embedded chip that will contain facial biometric and biographical data. The State Department expects that by the end of 2005, there will be 162 million Americans with these new biometric passports.

---

[135] ibid, Sec.203 (V)(iv)
[136] ibid, Sec.403 (c)
[137] "Enhanced Border Security and Visa Entry Reform Act of 2002," Sec.202 (a)(4)(A), < http://0-web.lexis-nexis.com.luna.wellesley.edu/congcomp/document?_m=d00982c906bc226d8daaa2df48afac73&_docnum=5&wchp=dGLbVzb-zSkSA&_md5=ba58ad0f749217a7abf6358228f28ede>
[138] Congressional Research Service. "CRS Report for Congress, U.S. Visitor and Immigrant Status

This US-VISIT program is being run by the Department of Homeland Security and not only requires the initial capture of biometric information upon application, but also upon entry and exit from the United States for all foreign visitors. In addition to providing identity verification, this information also allows the government to be easily alerted if a visitor overstays their allotted time. One positive aspect of the US-VISIT program is that it also created a redress policy to allow people to amend or correct data that is not "accurate, irrelevant or timely".[139]

However, this policy also expects any response to such a request to take up to twenty business days, which makes it very difficult for people to have their situations addressed in a timely manner. The Electronic Privacy Information Center (EPIC) directly addresses the privacy concerns brought about by the US-VISIT program, namely what would happen to the information of people who became United States permanent residents or citizens and then fell under the protection of the Privacy Act and that the Department of Homeland Security should observe the international standards of privacy set in the Universal Declaration of Human Rights, which state that no one "shall be subjected to arbitrary interference with his privacy" or that any "distinction shall be made on the basis of the political, jurisdictional, or international status of the country or territory to which a person belongs".[140][141] The most important concern that EPIC brings up, however, is that ability of the US-VISIT program to use the personal information collected for purposes other than that of the original intent of the program.[142]

Concerns

Biometric technologies raise a huge number of concerns from privacy and civil rights groups such as the Electronic Freedom Foundation, the American Civil Liberties Union and the Electronic Privacy Information Center. A prominent issue these organizations are concerned with is the ability of biometric systems to track people. In particular, that tracking information could be stolen or leaked to criminals or terrorists, which could lead to further problems. In addition, the knowledge that such tracking is taking place could also restrict the freedom of movement for people who are unwilling to be watched at all times.

Biometric information can be easily combined with that of other databases. In addition, such information is hardly foolproof. For example, if a person were tracked to an area of ill repute, then it would not be appropriate for the information to be used to assume that the person frequents these areas or is in any way connected to anything illegal.

Indicator Technology Program," RL32234, p. 8 < http://www.epic.org/privacy/us-visit/crs_us-visit.pdf>

[139] US-VISIT Redress Policy, <http://www.dhs.gov/dhspublic/display?theme=91&content=3776&print=true>

[140] Department of Homeland Security. "Docket No. BTS 03-01," p.3

[141] United Nations, Universal Declaration of Human Rights, G.A. Res. 217A(III), U.N. GAOR, 3d Sess., U.N. Doc. A/810 (1948), art. 12, reprinted in M.Rotenberg Ed., The Privacy Law Sourcebook 2003 318 (EPIC 2003)

[142] Department of Homeland Security. "Docket No. BTS 03-01," p. 5

Criminals may find ways to circumvent the system to avoid detection and the capture of their biometric information and circumvent the intent of the sensor system. Indeed, with such an increase in the dependence on technology, people will focus on finding ways to avoid the biometric sensors and evade them.

The disclosure of personal biometric information to third parties would ruin the anonymity of the customers. In the futuristic world shown in *Minority Report*, iris/retinal scanners are used to personalize advertisements. This, too, is an invasion of privacy for a person would no longer be able to shop or wander in a public place anonymously.

Lastly, it is difficult to provide effective notice of such surveillance mechanisms or to do so without defeating the purpose of such surveillance. For example, it is difficult for security measures to be effective with such notice. However, it would be an invasion of privacy for facial recognition systems to be used on streets to identify the customers of competitors in order to encourage or harass those customers.

The Electronic Freedom Foundation brings up seven more concerns that are directly related to biometric surveillance. Their first major concern is that biometric surveillance is inherently individuating. Since biometric identifiers are designed to identify a person exactly, there is no way that such surveillance does anything but identify individuals and therefore is capable of picking individuals out of a crowd.

Biometric surveillance interfaces easily to database technology. In fact, such database technology does present a great danger for privacy violations, which are not only made easier, with all of the information stored in one place, and more damaging if the information is able to tampered with and changed. This is of even more concern because biometric information is so individuating that it becomes very difficult to change if there is a mistake in the information.

The information that can be gathered from biometric surveillance is not a substitute for the intelligence information gathered from the traditional sources. The Electronic Freedom Foundation supports this statement by stating that the identification of criminals does not give away information about their activities or the means of preventing any future crimes. While this statement is true, the tracking capability of biometric surveillance does allow law enforcement to follow criminal activities though unable to prevent future crimes.

Biometric information is only as good as the initial identification. However, this also makes the biometric surveillance vulnerable for if a person's biometric identifier were mistakenly given to another person, it would become quite difficult for either person to prove whom they are. In addition, a person could purposefully give a false identification with their biometric information and, therefore, could be given false

access or able to evade law enforcement tracking and identification. Biometric identification can also often be overkill for the task at hand. For example, at a bar customers are required to show identification to prove that they are of legal age. However, there is no need to require biometric information with an identification card in order to prove identity. Thus far, though biometric identifiers may be a more secure level of identification, there needs to be a demonstrable need for such identifiers to be integrated with common identification.

Biometric identifiers, as the Electronic Freedom Foundation suggests, are also discriminatory. Certain identifiers, such as fingerprints, are discriminatory in the sense that certain genetic dispositions, such as people with chronically dry skin, have a greater difficulty in having their fingerprints read properly.

The accuracy of these surveillance systems is difficult to assess before deployment. However, there have been several studies done that demonstrate the effectiveness of certain systems. While further testing should be done, it is beginning to a concrete proof of any given biometric system's accuracy that such studies are being done and though the deployment of such systems is the only sure test of such accuracy, the studies can test the systems as much as possible.

Lastly, and perhaps of greatest concern, is the cost of failure of the biometric systems. One of the greatest problems of biometric surveillance systems is that if there is a mistake in the database such that a person is associated with the wrong biometric identity, then it becomes very difficult to prove such a mistake.

These concerns demonstrate that the activeness of the biometric systems has the potential to adversely invade one's anonymity. Any great over-processing of the information and distribution of the biometric information could lead to a loss of privacy and an increase in identity theft.[143]

Another civil rights group, the Electronic Privacy Information Center, has slightly different concerns than the Electronic Freedom Foundation. The greatest concern that EPIC brings up is the length that the government and private sectors will keep their information.[144] This is a concern because the information could be continually accumulated and used for purposes other than originally intended and with little thought to privacy or civil liberties.

In addition, such surveillance also requires repeated surveillance since it requires an initial capture and subsequent ones as well. This also means that there will be fairly regular transmissions between the sensors and the database in order to process the data. This means that the privacy intrusions will be constant and should be restricted in order to protect a person's anonymity and privacy in public spaces.

---

[143] Anonymous. "Biometrics," <http://www.eff.org/Privacy/Surveillance/biometrics/>

[144] Anonymous. "Concern Over Biometric Passports," 30 March 2004, BBC News, <http://news.bbc.co.uk/1/hi/technology/3582461.stm>

The distinction between voluntarily being caught by sensors and involuntarily doing so. This, however, can be addressed by placing security as a reason to require involuntary sensors; however, unless a full explanation can be given, sensors should otherwise remain voluntary in order to protect the privacy of the people.

The theft of information by others has the potential to greatly impair the victim's privacy. However, this has been partially addressed by legislation already. With our proposed Public Anonymity Protection Act, we simply aim to continue to address this issue as it already has been by the government by requiring the greatest technological security available for these systems and punishing violations with both criminal and civil penalties.

The next concern is database security. Since this information is personally identifiable, EPIC also is concerned that it is crucial to safeguard such large and valuable collections of information. In addition, it is true that these databases also need to maintain both reliable and up-to-date information in order to accurately identify users.

EPIC's last concern is that the information will be used to track users at each point that they make contact with the sensors. This issue should be addressed because the privacy of the people to use information that was declared to be used for one purpose has now been subverted for other applications without any consent by those parties who stand to lose their anonymity.

Having examined the concerns of the Electronic Freedom Foundation and Electronic Privacy Information Center, it is easy to see they had many of the same concerns. One of these concerns is the increase in the visibility of individual behavior. Our framework considers this concern to be a great impingement on the privacy of the people since it will prevent people from behaving freely which is certainly a restriction on a person's rights.

Such information, being used for both tracking and information could be used to produce both politically and personally damaging information. As in the example of the E-Z pass case where the information was used to demonstrate the infidelity of a partner in a divorce case. Biometric surveillance information could easily be used in the same way and in a similar manner. This is also a consequence that must be able to be limited in order to protect personal information and the desired privacy of the users. This will also some beneficial consequences, such as the capability of increasing the power of "circumstantial evidence" in criminal prosecution by being able to place both guilty and innocent people near a crime and track the movements of the people before and afterwards.

Information will be used to create behavior patterns that will be used as standards with which to compare individual's behavior and be used to make judgments and generalizations about people from this.

However, there is yet another beneficial possible consequence to biometric surveillance systems, such as the ability to aid in tracing missing individuals and making it much easier to locate them. In comparison to other surveillance systems, biometric systems possess certain benefits such as no need for a physical token that can be easily lost. However, this also makes it more difficult to change or revoke such a biometric identity. In order to protect the privacy and anonymity of people while allowing security concerns to be fully addressed, there are certain policy recommendations that, if followed, will allow the right to privacy to be protected in a public space while allowing security concerns to be addressed.

The major policy recommendations that address the concerns of the civil rights organizations deal, in large part, with the security of the databases on which the biometric information will be stored. In particular it is believed that it is necessary to create specific protocols to handle what information is authorized to be collected and kept in the databases and that reasons to support this collection of information should be disclosed to the public. In addition, there must be protocols addressing how long this information may be retained and under what conditions this information will be distributed. In order to limit the distribution of the information, the databases should be made secure and access should be restricted. Under our framework analysis, these measures will help prevent biometric surveillance systems from becoming even more active, though they are demonstrably inherently active. The Public Anonymity Protection Act deals directly with these concerns while also providing law enforcement agencies and the public sector the ability to use these sensors for security and other necessary purposes.

Policy Recommendations

In dealing with the government and public entities such as the Department of Homeland Security and the Federal Bureau of Investigation, section three of the Public Anonymity Protection Act clearly deals with the policy recommendations outlined and the concerns of the civil liberties organizations.

Any surveillance system needs to have a purpose that is clearly defined and that any information collected must pertain to this purpose and no additional information may be collected and stored. In addition, this section requires the public notification of the nature of the data being collected and the ability to change or alter the information so that a person is able to ensure the accuracy of his own personal information.

Another crucial part of this section is the establishment of an auditing body that will be able to ensure that all of the government surveillance programs adhere to the policies outlined in the Public Anonymity Protection Act in order to guarantee that the government is stepping over the boundaries of a person's right to privacy and anonymity.

The second part of section three of the Public Anonymity Protection Act also addresses the concerns of the civil rights groups by limiting the government's ability to retain the biometric information any longer

than original stated or unless significant reason was given that demonstrated the necessity of holding the information longer than originally intended. This also prevents the government from over-processing the information in order to mine it for further personal information that is not compliant with the original purpose and intent of the system nor allow the distribution of the information to any third parties. This section of the Public Anonymity Protection Act not only addresses the concerns of the civil rights organizations, but it also allows the law enforcement agencies to continue using both new and old technologies in order to use surveillance for security and identification purposes.

This act does not prevent any government agencies from continuing to use information-collecting technologies, especially for any purposes deemed necessary for the security and safety of the American people. However, it also provides protection to the people in order to prevent the government from collecting unnecessary personal information that could be used to infringe on a person's rights to privacy and anonymity.

The Public Anonymity Protection Act also covers protection from the private sector. However, this protection is approached in a different manner in order to provide private entities the right to protect their own property as well. In addition, most concerns with the abuse of the information obtained from biometric sensors are connected to the government because of the government's greater capabilities and needs to deploy such systems. Therefore, using the tort system in order to allow individuals to seek redress for any intrusions upon their privacy and personal information allows individuals to address their privacy concerns whenever they feel as though they have been abused. This means that private entities are not forbidden from collecting, storing, processing or distributing the information collected.

However, the Public Anonymity Protection Act does restrict private entities from collecting information in an illegal manner or without the permission of the person. In addition, it also hold the private entities liable if the information gathered is false or processed such that it construes personal information in a false light in order to protect a person's identity and character. This part of the Public Anonymity Protection Act also protects against the unwanted disclosure of this personal information to third parties, which will help prevent the accumulation of large databases of information that could be over-processed and mined to create large collections of personal information. This section of the Public Anonymity Protection Act allows private entities to pursue such surveillance and collection of biometric information as they desire, but also provides limitations on the over-processing and distribution of the information, in addition to providing the people with a way in which to prevent the private entities from accumulating more personal information or invading their privacy and anonymity without any reprisals.

Conclusion

By applying the analysis framework we have developed to the area of biometric surveillance in public spaces we have shown that biometric surveillance is an active form of surveillance where the data is not

only accumulated but requires storage and processing as well. Unlike many other forms of surveillance, most biometric surveillance is an opt-in procedure that requires giving a biometric identifier and personal information in order to obtain the possible benefits of such a system, such as the National I.D. cards or the biometric passports that are being implemented. In addition, the framework has demonstrated that biometric systems are becoming much more common, which has been demonstrated by the increase in the size of the industry. As the technology has become more affordable and easier to use, it also makes economic sense to replace the security guards and other anthro-equivalent positions with biometric sensors. For these reasons, it seems as though biometric sensors and surveillance are becoming even more active and as they become more pervasive, it is important to protect the people's privacy and anonymity while allowing both the government and private sectors to continue using biometric surveillance for security and other necessary purposes.

In order to respond to these concerns and needs, we have created the Public Anonymity Protection Act to created the necessary restraints that will protect privacy in public spaces while still giving both public and private entities the ability to continue using biometric technologies for surveillance. This act restricts the government more than private entities, which, for biometric surveillance, makes sense since most of the concerns with biometric surveillance are with the government's ability to combine both personal information and biometric identifiers into a large collection of information. In particular, these large collections of information will have to be stored on databases that are vulnerable to attack so it is necessary to restrict the government's storage and distribution of such data while ensuring that the databases are protected to their fullest ability. On the other hand, private entities are less restricted on their collection, storage, processing and distribution of such biometric information. However, under this act, they are considered liable to the people for any invasion of privacy, misuse of the information and the unwanted distribution of the information. This alone will create a disincentive for companies to collect more information than is necessary and to ensure that the information is correct and secure in order to avoid any redress and lawsuits by the people. By using our analysis framework, we can not only understand where biometric surveillance lies in the spectrum from passive to active forms of surveillance, but we have also been able to create an act that is capable of dealing with the concerns of the civil rights organizations while simultaneously providing both the public and private sectors with the necessary ability to use biometric surveillance as deemed necessary.

Internet as a public space

The Internet is as much a public space as any park, street, or other areas where there is open access incorporates public behavior, visibility, large quantities of people and promotes assembly. The Internet may be viewed as a technological medium rather than a physical medium because two feature capabilities are easy access to instant information and global data. Individuals using this medium often have a greater expectation of privacy than the technology or law currently allows. There is an increased

need to raise awareness of serious issues that affect individual's privacy and anonymity in both the electronic and physical world.

Characteristics of a public cyberspace

The Internet has characteristics of a public space, but it is important to note that we are not classifying the whole cyberspace world within the realm of public space. The Internet consists of public space, private sector space, and personal space, but since the "public space, private sector space, and the personal spaces merge seamlessly," we evaluate the Internet to address public space concerns in anonymity.[145]

Examples of public space on the Internet include chat rooms, message boards, blogging, and forums. These spaces all encourage public behavior.[146] Hence, the Internet embodies a public space attribute. Andrew Shapiro and Jerold Kayden believe the Internet can "incorporate a democratic public forum characteristic of public space with its diversity and fortuity."[147] An example of this is the Library Forum initiative whose goal is to "protect one of the last truly public spaces [the library]."[148] The library forum is an example of public space on the Internet. It offers 24-hour open online access to an abundance of information in articles and digital collections. Helsinki's library is part of this forum, and it encourages online face to face meetings, debates, and discussions.[149] Online meetings through this library offer a parallel from meetings in physical places. Therefore Internet spaces encourage public behavior and allow the Internet to become a place for information commons.[150] The Internet has become a vast space that "reflects diversity and encourages free speech and creativity."[151]

In our study of Internet privacy and anonymity concerns in public space, we study areas where a) public behavior constitutes the main activity, b) types of technologies on the Internet primarily monitor individuals on the networks, c) where personally identifiable information is easily accessible, and d) distribution of unwarranted information is made widespread due to the distributive capabilities of the Internet.

---

[145] Jean Camp and Y.T. Chien. The Internet as Public Space. 30 Oct 2004, John F. Kennedy School of Government, Harvard University, <http://www.ljean.com/files/spaces.html>

[146] ibid

[147] Jerold Kayden and Andrew Shapiro. "Is Public Space Dead?," Fall 1999, <http://www.vanalen.org/forums/public_space.htm>

[148] "Future Library Forum: The New Helsinki Central Library," <http://www.aula.cc/projects/futurelibrary/newlibrary.html>

[149] Howard Rheingold. "Helsinki's Aula," 17 July 2002, <http://www.thefeature.com/article?articleid=15435&ref=4529009>

[150] Camp.

[151] Howard Besser. "Intellectual Property: The Attach on Public Space in Cyberspace," 28 Oct 2004, UCLA School of Education & Information, <http://www.gseis.ucla.edu/~howard/Papers/pw-public-spaces.html>

Analysis Framework

We analyze the technologies of the Internet using our analysis framework. To consider how the technologies on the Internet bring up privacy and anonymity concerns, we look at the setup of the Internet—that is the network and infrastructure that the Internet is so dependent on. Below there is a summary table and a visual representation of our identification potential spectrum for the Internet.

	Internet as a Public Space on the Analysis Framework
Human Functional Equivalent	None.
Opt-in or Opt-out	Some options available, need more.
Pervasiveness	Yes.
Personally Identifiable	Yes. Information found on the Internet can be personally identifiable, and often have no access restrictions.

Table 8: Summary of Application of Analysis Framework in evaluating anonymity and privacy concerns on the Internet.

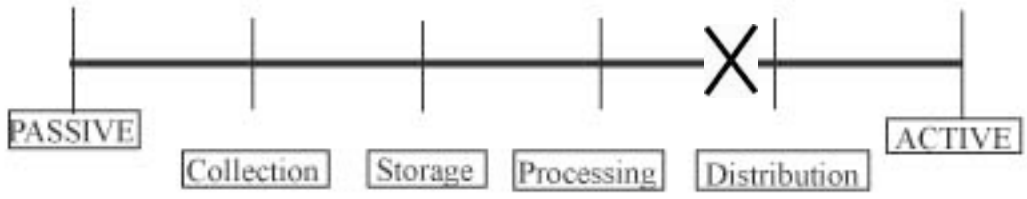

Figure 6: Internet is best placed at the more active end on the Identification Potential Spectrum. The Internet is capable of being anywhere on this spectrum with its capacity to collect, store, process, and distribute information. However, the Internet is most powerful in transmitting information, or distribution of data (in bits) over the networks. The distribution capabilities of the Internet push the overall Internet as a public space toward the active end of the spectrum and increase the need for anonymity and privacy protections.

Human Functional Equivalent

Overall, it is hard to find a human functional equivalent of the Internet due to human limitations in combining and distributing information. The Internet does not have a human counterpart. The network infrastructure of the Internet cannot be manned by one person. The Internet survives because there is no one person in charge of the whole network. Rather, it is made up of computer networks which are inter-connected using the Transmission Control Protocol (TCP) / Internet Protocol (IP) communication protocols, with domain name and IP-address assignments provided by the Internet Assigned Numbers

Authority (IANA) and the Internet Registry (IR).[152] While there is a common naming system, no one is in charge of the content and gathering of information on the Internet. If a human cannot have complete control over the environment (domain), then whatever monitoring or sensing is done on the Internet has no human functional equivalent.

Consent

There are some situations such as tracking programs that necessitate consent using opt in/out options to ensure privacy and anonymity protection. Much of the monitoring done on the Internet (of chat rooms for instance) is not prerequisite for accomplishing a job function. Hence, the ability to have opt-in or opt-out exists. The technologies that allow for such options must be extensible to all platforms so that all users can benefit from such a choice.

Pervasiveness

In general, the Internet fosters pervasiveness, which requires PAPA to make recommendations to make it harder for information to be readily available online. The technologies the Internet uses to disseminate information make it very pervasive. As the Internet becomes the dependent source of obtaining information, the technologies used, for example the networks that carry the information, the servers on which hosts operate, and the firewalls that aim to protect privatized networks, are being used even more. This includes HTML and JSP technologies which allow information to be posted or displayed online. Many businesses are coming up with premade packages to allow more people to make their own webpage (i.e. Yahoo), start their own Xanga journal, or create their own blog. As technologies make information transmission more common, it becomes harder to regulate such pervasive technologies to restrict the information that is passed along.

The transmission medium is also changing and making an Internet connection much more pervasive. Technology offers many options in getting an Internet connection. You can be connected to the Internet by dialing up using telephone line, a local-area network (LAN), data cables, or high speed digital subscriber lines (DSL). In the past couple of years, wireless technologies embedded in a WiFi card transmit radio signals using base stations. These wireless base stations are becoming more and more prevalent in public spaces, such as restaurants, hotels, and libraries.[153] Also, technology is being developed to allow broadband Internet services to be accessible through basic power lines.[154] This makes Internet connection possible through basic energy power lines. This is another step closer the Federal Communications Commission's (FCC) goal of universal broadband service. Cable does not have universal coverage, but power lines do, meaning rural areas are a new market for broadband Internet

[152] Clarke, Roger. "A Primer on Internet Technology," V. 15, 19 Feb 1998, Australia, <http://www.anu.edu.au/people/Roger.Clarke/II/IPrimer.html>

[153] Marshall Brain. "How WiFi Works," 2004, Howstuffworks, <http://computer.howstuffworks.com/wireless-network3.htm>

[154] Anonymous. "Plugging in, at last.," The Economist Technology Quarterly. The Economist, Vol 373, No. 8404. 4 Dec 2004. p. 3-4. XXX "Big Brother." *The Economist*. Dec 2004.

services.[155] It is becoming easier to use the Internet because the types of medium used to transmit information are more and more accessible to the general public. We went from the common telephone line to cable to improving the telephone line for DSL.

With the continuing development of technologies with the Internet, pervasiveness on the Internet has increased. There is a growing concern of protecting anonymity and privacy to limit the information transmitted by pervasiveness technologies on the Internet.

Identification Potential Spectrum

The Internet has the capability to collect not only identifiable information collected by other technologies but can also collect location information as well as digital information. Location information is an IP address that can be used to locate an Internet user. Digital signatures are a form of digital identifying information. While it is acceptable at times to collect such personally identifiable information, there are instances when too much information is being collected and processed. We look at different stages on the identification spectrum when such information from the Internet raises privacy and anonymity concerns. We focused on these four parts of the Internet in the rest of our analysis and case study examples: 1) chat rooms, message boards, blogs, forums; 2) private sector or company websites; 3) personal or individual websites; and 4) online government public records.

The Internet lies on the more active end of the spectrum in regards to most information. (Figure 7). A lot of information available online is personally identifiable, not anonymized, and not encrypted. From case studies to be discussed later in the Internet section, we look into how the Internet not only facilitates collection and storage of information in databases and on the networks, but also makes it much easier to process identifying information and distribute it all over the network.

Collection

There are three types of personal information collected from the Internet: personal identification, location, and digital information. Digital information refers to information embedded in digital signatures and encryptions that allow for identification.[156] Personal identification information is the most basic of information collected on the Internet. It includes information a user inputs about himself upon a website or company request. Examples of personal identification information include name, address, social security number, contact phone number, instant messenger screenname, etc. Location information encompasses the physical location of the user, the IP address that can give the computer location, and can be tracked over Internet domains. Personal identification information collected on the Internet usually requires consent from the user inputting the information. Location information can usually be obtained without consent from the user. Once you log onto a computer, your username and domain are broadcasted and an IP address is the location label. It is important to also note the purpose for data

[155] The Economist. 4 Dec 2004. p.3.

collection on the Internet. There are many instances where the information is used solely for marketing purposes. The Internet has not only increased the amount of data collected but has made it much easier to collect data and to recollect data whenever there is missing information or mismatching information. In our case studies, we looked at how much information is acceptable when collecting data online and propose methods to limit the amount of information collected.

Storage

Storage of information on the Internet brings up additional concerns in privacy and anonymity. There is little to no consent from the individual in storage of personal information. Data collected from a marketing survey is automatically entered into a database, without prior notification of the consumer. Information is most likely stored in online databases, but there is very little transparency in the method and location of storage. There is little transparency because users do not know where their information is being stored nor how their information is being stored. Typically, online databases are not made available to end users, so these individuals cannot check the legitimacy of the information presented, thereby having no transparency. Additionally, the ease of online databases in combining information raises many anonymity concerns. If databases cannot isolate the information, shared information increases the chance of personal identification, hence a loss of anonymity. Databases lack transparency and are easy to combine, which make storage of personal information susceptible to violations of anonymity and privacy.

Latanya Sweeney from Carnegie Mellon University has proposed the k-anonymity model that would protect databases before they are shared.[157] The model addresses anonymity concerns that arise when databases are shared. The k-anonymity model uses an algorithm that can generalize the images then uses cryptography to lock the images. Each individual record is minimally generalized so that it indistinctly maps to at least k individuals, where k is defined by policy and security. Although the k-anonymity model is not a 100% guarantee that individuals cannot be identified, it provides an effective safeguard against unnecessary identification of most individuals. Some real-world systems such as Datafly, m-Arguys, and k-Similar use this as their basis of anonymity protection.[158] This model looks into the protection of anonymity and protection of databases before sharing or merging occurs.

Processing

Data processing on the Internet raises heightened concerns in privacy and anonymity because it oftentimes allows for information to be compiled in a way that may reveal identities of individuals when the information was originally anonymous—the k-anonymity model shows one way of protecting information. Processing can result in identification of individuals in public space. Most of the data processing on the Internet skips over consent, with the exception of fee-based services for finding

---

[156] Anonymous. "Digital Identification." <https://digitalid.verisign.com/server/about/aboutFAQ.htm>
[157] Latanya Sweeney. "k-Anonymity: A Model for Protecting Privacy.", May 2002, Carnegie Mellon University, <http://privacy.cs.cmu.edu/people/sweeney/kanonymity.pdf>
[158] M. Granger Morgan and Elaine Newton. "Protecting Public Anonymity," *Issues in Science and*

personal information on individuals. Some of these sites such as peopledata.com explicitly note that they combine online databases of information to come up with a report on an individual. However these private services do not require an individual's consent for release of personal information. There is currently an abundance of data processing, but is there a real need for so much data processing? One method of reasoning is to look at data processing for infrastructural functionality. We differentiated between infrastructure functional data processing with noninfrastructure functional data processing. Data processing is then acceptable only when processing collected data is essential for Internet infrastructure. For example, an IP address is functionally useless unless it is processed to determine the physical location of the machine on the network. The infrastructure of the Internet requires that an IP address be processed to locate the machine. However, data processing is not infrastructure essential for marketing studies which use collected information. The information processed from the marketing studies (often times collected by monitoring agents or cookies) is not in any way related to the Internet infrastructure. It is merely, personally identifiable information.

Technology capabilities of the Internet have made it more convenient to process data, especially data stored in online databases. However, through our research we have aimed to hold the abilities of technologies to the standards of non-technologies. It is not acceptable to process more data out of convenience through technological means. One of the ways anonymity is protected in PAPA is restriction in data processing.

Distribution

The Internet offers a powerful mechanism for distribution of information. In fact, distribution of data is singly the most powerful threat to privacy and anonymity concerns. The Internet is a "superhighway."[159] More information is passed over the Internet than any other communication medium- whether that be television, radio, satellite. Whether over public, private, or personal spaces, the Internet broadcasts information over all cyberspace. Therefore, if private information is available on the Internet, it can be easily distributed to everyone who uses the Internet. Currently there are security checks such as personal certificates and encryption in place that protect some private information. In later examples, we demonstrate how there are other private information that is being broadcasted all over the Internet, even with encryption technologies. Data protected by personal certificates or available on blogs involve user consent. But this is not always the case, as we will see in later examples. Some private information is disseminated without user consent, leaving users no choice in the protection of their personal information. PAPA outlines what is appropriate distribution of information.

Values

We consider similar values and protections on the Internet and other physical spaces. This includes First

---

Technology, Fall 2004, p. 83-90.

[159] Anonymous. "Unfortunately, the Surveillance Superhighway is here. Now!," 28 Oct 2004,

Amendment freedoms such as the freedoms of assembly and speech. We are concerned with the privacy of personal information submitted, received, and processed. We look into a possible expectation of privacy and expectation of anonymity on the Internet. Moreover, we aim in our proposed legislation to maintain anonymity when information is passed through networks. We put the Internet through our identification spectrum and analysis framework. Now we consider the values and protections of anonymity and privacy in specific case studies.

Case Studies

We looked at four different case studies that bring up different privacy and anonymity concerns on various parts of the spectrum. The case studies are an advertising company called DoubleClick.com, online government public records, the Cyber Patrol initiative by the Securities and Exchange Commission (SEC), and the University of Berkeley "Demonstrate" surveillance project. Each case study looks into more detail one of the four areas with privacy and anonymity concerns specified in the introduction of the Internet as a public space.

In our study of Internet privacy and anonymity concerns in public space, we study areas where a) public behavior constitutes the main activity, b) types of technologies on the Internet primarily monitor individuals on the networks, c) where personally identifiable information is easily accessible, and d) distribution of unwarranted information is made widespread due to the distributive capabilities of the Internet.

DoubleClick.com

This case illustrates a technology that primarily monitors individuals on a part of the Internet. DoubleClick.com is an online advertising company that places third party advertisements on websites.[160,161] A cookie, or an electronic tag, is placed when a user clicks on one of the advertisements. The cookie then follows the user around the web, storing information of the whereabouts onto the user's hard drive.[162]

DoubleClick's sole purpose for collecting the data is for marketing reasons to increase profit margin. It created anonymous Internet profiles with each user. Then in 1999, DoubleClick.com acquired Abacus Direct, a direct mail company with personal information databases. This caused uproar among privacy rights activists.[163] The acquisition of Abacus allows DoubleClick to personalize the "anonymous" profiles

---

<http://wearcam.org/visualfiltervidescrow.html>
[160] DoubleClick.com. <http://www.doubleclick.com>
[161] Privacilla, <http://www.privacilla.org>
[162] Anonymous. "What is a cookie?" <http://www.webopedia.com/TERM/c/cookie.html>
[163] Courtney Macavinta. "Privacy advocates rally against DoubleClick-Abacus merger," 22 Nov 1999, CNET News, <http://news.com.com/Privacy+advocates+rally+against+DoubleClick-Abacus+merger/2100-1023_3-233413.html>

through database sharing.

This is a case that shifted DoubleClick from the passive side to the active side of the spectrum after the merger. Before the merger with Abacus Direct, DoubleClick.com collected location information from the user by tracking its mouse clicks on advertisements. It stores the information in anonymous profiles, with careful attention to maintain anonymity. The purpose of the information is for marketing. The information collected can theoretically be done by a human functional equivalent. Someone can in fact keep track of the advertisements observed by groups of users, but is much harder and technology provides a more efficient means of accomplishing the marketing goal. There is no opt in/out procedure for consumers; they are automatically being tracked by DoubleClick.com. Since the profiles tend to be used only for company marketing strategy there is a small threat of pervasiveness. The information is not identifiable, because it is anonymous.

However, the merger with Abacus Direct shifts the company on the identification spectrum. The information collected and stored by DoubleClick.com does not change but there is high probability for data processing. Databases from Abacus have personal identification information. Profiles from DoubleClick.com have anonymous location information. Combining the data from these two sets of information obscures the anonymous barrier of DoubleClick.com. With personal information from Abacus, DoubleClick can now create detailed, personal profiles of a user's name, address, tracking history, and other pieces of information. The information is more identifiable after processing the data (merging databases) because there is more information to use to identify an individual. Although DoubleClick.com had no immediate plans for distribution of information, the merger with Abacus Direct brings up privacy and anonymity concerns in the active data processing part of the spectrum.

This case study focuses on the security of information obtained from databases. In database storage, it is important to keep database information isolated so that there is less likelihood of linking personally identifiable information together. The Internet has a lot of data stored in different databases on various parts of its networks and processing data from multiple databases takes away the anonymity proclaimed by each individual database. There exists a need to protect anonymity on the Internet and PAPA includes recommendations for maintaining separate storage spaces to restrict data processing in order to protect consumer and individual anonymity.

DoubleClick.com, in response to outspoken privacy rights activists, offered a compromise agreement with ten states. It promised to maintain the anonymity of consumer information but gave consumers access to compiled profiles and allowed consumers the ability to opt out of its Internet tracking service.[164] Their current privacy policy is a model example of what other Internet companies can do to accomplish their business goals (here it was collecting information for marketing purposes) while addressing privacy needs

[164] James C. White. "People, not Places," Spring 2003, p. 20.

of their consumers. Their agreement emphasized that anonymity of consumers was important on the Internet. In addition, the ability to opt-out places gives the consumer choice in deciding whether or not the personal information should be collected and used by DoubleClick.com. The current privacy policy includes three important points:

- "No personal information is used by DoubleClick to deliver Internet ads..";
- "You [the consumer] can control the technologies used to collect information during ad serving..Click here for the ad-serving cookie opt-out"; (Figure 9).
- "Transparency – We are committed to transparency about our practices and provide the links to the left for more information about specific DoubleClick products and services."

PAPA emphasizes what DoubleClick.com has done: elicited notice and consent, offered the ability to opt-out, maintained anonymity, and assured transparency of products and services.

	DoubleClick.com on the Analysis Framework	
Human Functional Equivalent	Marketing Analysts.	Post Merger: None.
Opt-in or Opt-out	None.	Post Merger: Yes.
Pervasiveness	No.	Post Merger: No.

Table 9: Summary of Application of Analysis Framework in evaluating anonymity and privacy concerns of DoubleClick.com.

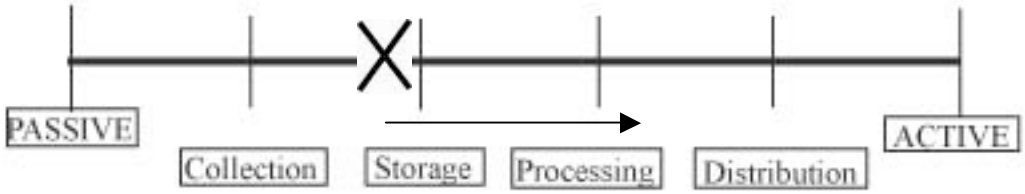

Figure 7: DoubleClick.com is best placed at the storage part of the identification spectrum, but the merger with Abacus has shifted it more to the active side, and toward data processing.

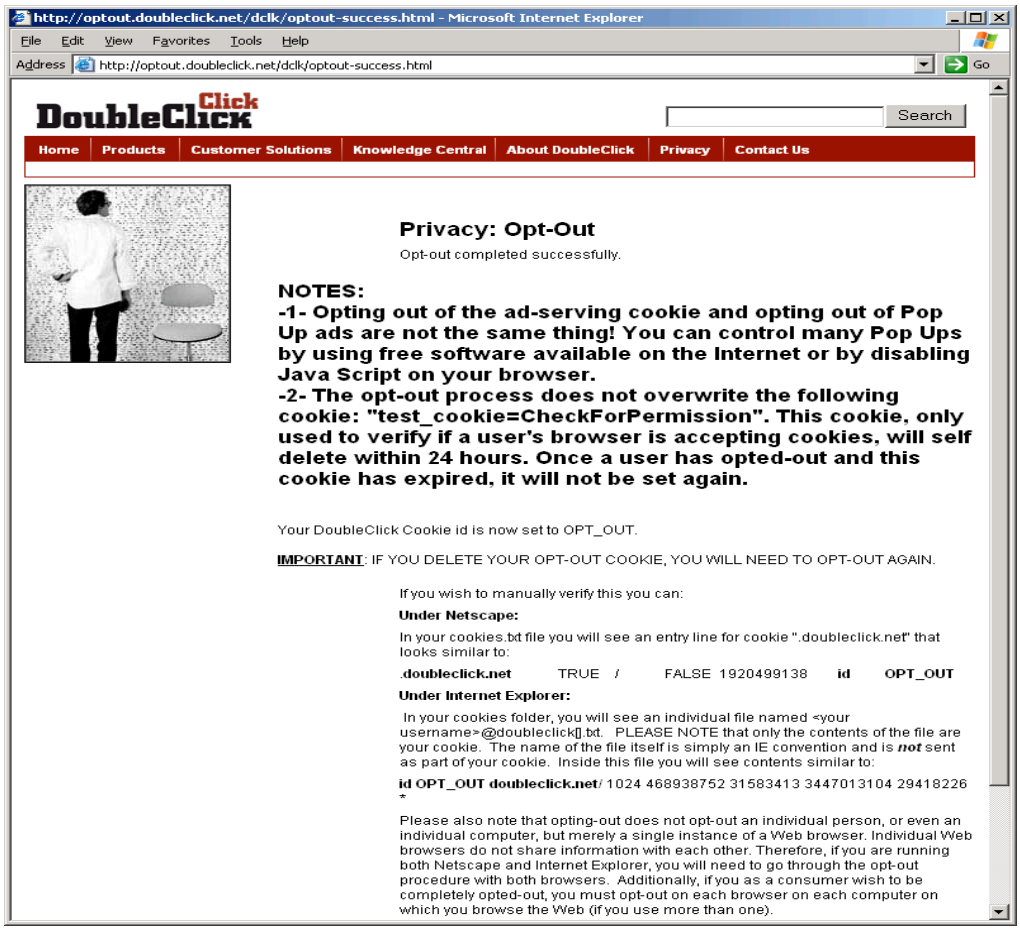

Figure 8: from doubleclick.com. Opt-out granted successfully.

Government Online Public Records.

This case illustrates how easily accessible personally identifiable information is online. Government public records are readily available to the public to offer transparency between the state and the citizen.[165] Before the Internet, these record archives would collect dust in the city courthouse. Now there is a movement for these public records to be put online for ease of access. Types of public records include and are not limited to motor vehicle records, court files, bankruptcy files, criminal records, registered votor files, and civil court recordings.[166]

Currently there are two methods in which public records can be accessed by online users. One is through posting on a government website. So the government-owned sites have these public records that people can request to see. The other method is access through fee-based private services where the government sells the public record information to these companies. These companies, in turn, make

[165] Beth Givens. "Public Records on the Internet: The Privacy Dilemma," 19 Apr 2002, San Francisco, CA, <http://www.cfp2002.org/proceedings/proceedings/givens.pdf>

it a fee-based service to obtain information from the public records. For example, Wisonsin's Department of Transportation received $8 million a year from selling motor vehicle records to these private companies. New York's motor vehicle department received $17 million one year from allowing public access to driver's license records.[167] The government should not be making any money by the sheer collection of public record information.

We consider online public records on the active side of the spectrum. Government public records unnecessarily distribute personal information. Records distribute information that has been collected by the government, stored in a government database, then processed by a private company to anyone who is willing to pay the fee. Finally, they are accessible via the Internet to nearly everyone. The Internet makes it easier to distribute information from these records to requested persons. The human functional equivalent goes back to having the records in the dusty courthouse guarded by government officials. There is no opt in/out procedure because public records must be kept on everyone. No efforts have been made yet to restrict *access* to public records. Online public records are pervasive, refer back to Figure X if needed. There is no identity check to see if the person requesting records is indeed the individual whose information is on those very records. However, public records do not have to be online. Having online public records make the information pervasive to everyone on the Internet. Public records should be made available for the individual, not for anyone with a credit card.

---

[166] ibid

[167] U.S. Supreme Court. "Janet Reno v. Bill Pryor," No. 99-61. <http://www.usdoj.gov/osg/briefs/1999/2pet/7pet/99-0061.pet.aa.html>

Figure 9: from webdective-online.com. The types of public records available online and accessible through a $29.95 service.

We tested the security of these public records by searching for public record information online, using one of the online services. In our test, we paid a fee of $45 to peopledata.com to obtain personal information on Hal Abelson, a professor at the Massachusetts Institute of Technology. It was a simple credit card fee transaction and within seconds, his personal information came up. (Figure 11). We were able to view personal information, date of birth, age, spouse, address, contact phone number, as well as a clear satellite image of his home. In addition, house value information and all similar information on neighbors were available. There was bankruptcy record check that came out negative, and a criminal background check that came out negative as well. So for only $45 we were equipped with a myriad of data on Professor Abelson.[168]

[168] Appendix.

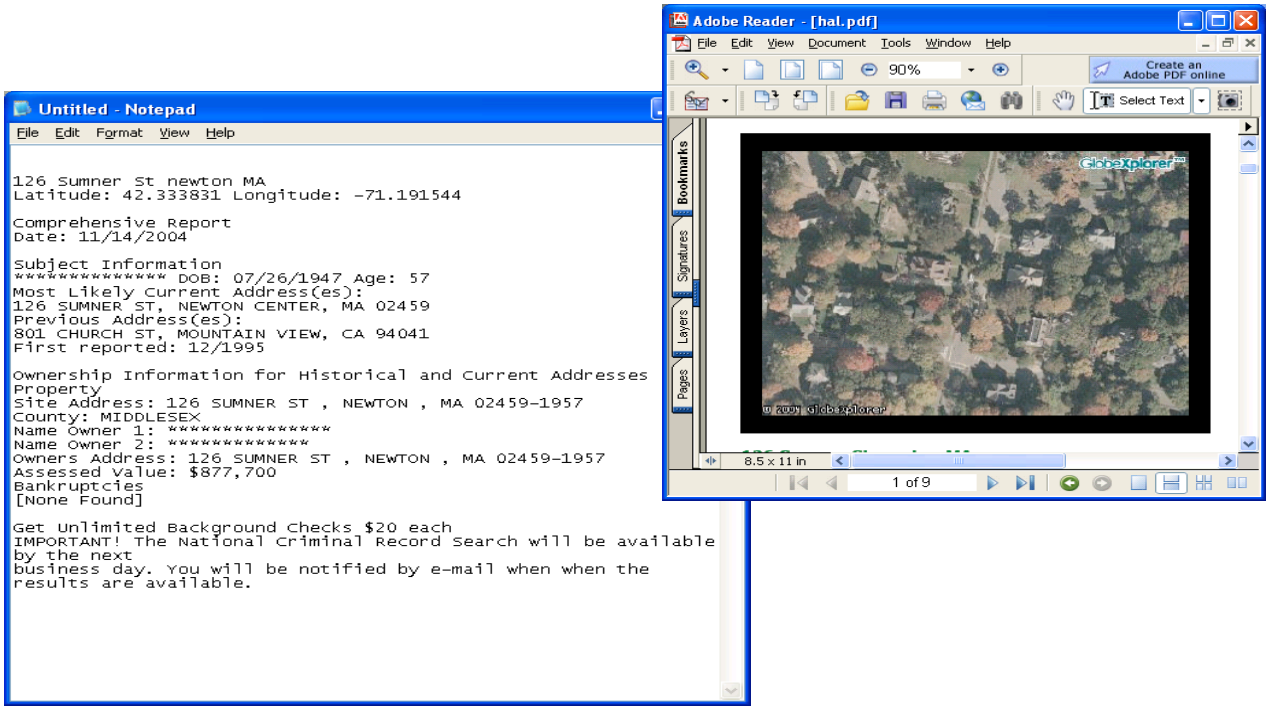

Figure 10: modified from Appendix. Personal information on Professor Hal Abelson obtained through peopledata.com, a fee-based people-finder service that uses online public records databases.

What can happen now? The information gathered and compiled from peopledata.com can be distributed with Professor Abelson's consent. This information can be used to find out additional information on Abelson through additional database processing. With enough information collected, someone can take Professor Abelson's identity and overcharge credit cards, conduct criminal activities under the new identity, track Abelson's activities and life because the information noted the exact address and image location of his residence, and more. The ease of access provided by the Internet in regards to online public records through search engines like webdetective-online.com and peopledata.com needs to be checked with a different set of regulations previously used to protect privacy with public paper records.

When the wrong person accesses the information on public records, extreme consequences can ensue. For instance, actress Rebecca Shaefer was murdered in 1989 by someone who found her address by going to the Department of Motor Vehicles with her driver's license information. Even after she took great precautions to keep her contact information unlisted, the murderer was able to obtain her records. The Driver's Privacy Protection Act (DPPA) was enacted in 1994 in response to this case. DPPA generally prohibits states from "disclosing personal information that their drivers submit in order to obtain drivers' licenses."[169] With new services on the Internet like webdetective-online.com and peopledata.com, it is clear that security and privacy will be compromised. Moving public records online makes it harder to check the identity of a person requesting a public record. There is nothing stopping identity theft.

[169] Anonymous. "Public Records," 21 May 2003, <http://www.privacilla.org>

The values this online public records case study needs to address are protection of personal information, access of public records, and anonymity. Protecting one's personal information includes accuracy of information. Access of public records includes protecting against identity theft and security of public records. Anonymity is important for online public records to create a level of abstraction between someone searching for private information and the database of personal records. In PAPA, we aim to address these concerns through our recommendations.

Recommendations for government public records include implementing a two-tier system of information, restricting access, requiring consent by the individual, and anonymizing individual information by creating aggregate data.[170] These recommendations incorporate elements of PAPA. For instance, the two tier system limits information, and restricting access decreases the possibility of distribution. Anonymization of individual information into aggregate data protects individual information from being distinguished.

Privacy activists believe that

> "the root of the problem with drivers' license records, and all public records, is collection of large amounts of data by governments in the first place. Requiring records to be kept secret treats a symptom of a larger disease…Individuals do not have a practical option of refusing to share information when they apply for a driver's license, so information collections should be strictly minimized. Once such information is in public record, the ability of the individual to keep it private is eroded…"[171]

The two-tier system has been proposed by some people for specific public records.[172] We looked at recommending a two-tier system to protect information currently available on online public records. We also considered at other legislative recommendations in various states. For instance, the Online Privacy Protection Act of 2003 (OPPA) mandated notice through a privacy policy and explicitly stated what was personally identifiable information online.[173] After a review of what some states have done in regards to public records, we believe the two-tier system offers the best of both records—sustaining democracy through government transparency yet allowing individual privacy of information.

We recommend a two-tier system to limit the amount of information displayed online. The first tier would have information accessible to the public, just as they currently are online. The information accessible would be information that would not reveal one's name or social security or any other extremely personally identifiable information. Criteria could be determined by Sweeney's k-anonymity model or by

---

[170] Givens.
[171] Anonymous. "Public Records," 21 May 2003, <http://www.privacilla.org>
[172] Laura W. Morgan. "Strengthening the Lock on the Bedroom Door: The Case Against Access to Divorce Records Online," Journal of the American Academy of Matrimonial Lawyers, Vol 17:1, 2002, p. 64.
[173] Online Privacy Protection Act of 2003 (OPPA), California Business and Professions Code § 22575-22579. <http://www.leginfo.ca.gov>

anonymization, to be described later. The second, more secure tier would require encryption and personal certificates to access. Therefore, only the individual whose information is on a particular record, *r*, can access record *r*. The personally identifiable information excluded fro the first tier would be accessible on the second, more secure tier. The extra step in security provides a buffer for access control.

Restricting access can include implementing digital certification through cryptography to only allow specified individuals access to data. It is possible to only allow individuals to access their own public record online. This makes sense, because its human functional equivalent is to go to the City Courthouse archive and dig up their individual record. Having the record online makes it convenient. The ability for 'instant access' at the "tip of your fingers" raises the concern that such user friendly options with the Internet may make it easier for people to access others' records.[174] But to ensure privacy of the record, if the online record is only accessible by the individual party, then Professor Abelson's information would not be available for our potential misuse. Additionally, we can allow an opt-in procedure where consumers can consent to have their records available online for the general public. We stress opt-in instead of opt-out because of the pervasiveness of the Internet. We want people to actively consent to have their records made readily accessible.

Anonymization of aggregate data would address distribution of private information online. This is especially important to do when the data will be used later for marketing purposes or company research. Currently, the FOIA grants company researchers requests for public records on individuals.[175] Although the information supplied to them usually involves some sort of anonymization, there is no set guideline to anonymize all aggregate data compiled. Anonymization of data will enhance protection of information for specific individuals.

	Online Public Records on the Analysis Framework
Human Functional Equivalent	Yes (courthouse marshall).
Opt-in or Opt-out	No.
Pervasiveness	Yes.
Personally Identifiable	Yes.

Table 10: Summary of Application of Analysis Framework in evaluating anonymity and privacy concerns in online public records.

[174] J.B. Shelleby. "Online court records raise privacy issues." 19 Feb 2003, *Ipswich Chronicle,* <www.townonline.com/ipswich/news/local_regional/ips_newiconlineje02192003.htm>Shelleby, J.B. "Online court records raise privacy issues." *Ipswich Chronicle.* 19 Feb 2003.

[175] Anonymous. "Freedom of Information Act Exemptions." <http://www.sec.gov/foia/nfoia.htm>

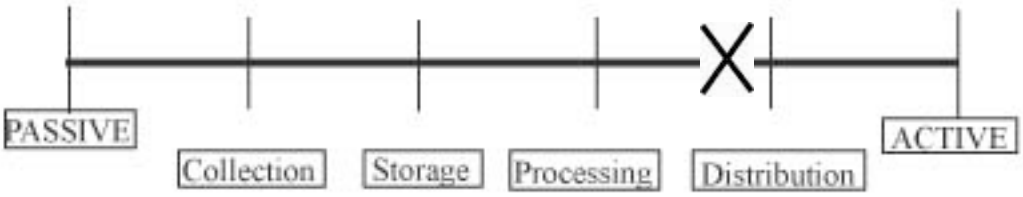

Figure 11: Online Public Records is best placed at distribution on the Identification Potential Spectrum.

Cyber Patrol Surveillance

This case monitored a place where public behavior constitutes the main activity. The SEC deployed the "Cyber Patrol" project in 1995 to patrol the certain spaces on the Internet everyday for fraudulent practices.[176] As of 2000, they had 240 people employed who combed message boards and websites everyday for illegal activity. They had found 125 cases for online fraud. The Cyber Patrol project falls under the more passive end of the spectrum. The employees merely collect data and evaluate (subjectively) the data. The data is stored but not for a long time, provided the case goes to court in a timely fashion. If a conversation from a chat room was posted on a website and it was about how someone tricked one bank website and withdrew money multiple times from their account but only got recorded once by the bank (i.e. 6.001 ATM example), then the Cyber Patrol employee used this information to prosecute the individual. The information may be stored in a database but not for any other use than to use the information in court; it will not be kept for later use in data processing or distribution. The information collected is being handled directly in court. It is hard, but not impossible, to find a human equivalent to this because it is hard to track online fraud without using technology. However, it is possible in that there can be someone checking up on every person using message boards and websites. Not likely, but still possible. Cyber Patrol did not offer opt in/out, but it is identifiable surveillance. This surveillance is not very pervasive because this project is limited by the 240 employees. The project is able to find out personal information linking to names of specific individuals and then bring up cases against them in court.

In a message board, a deemed public space on the Internet, is it right for such information to be collected and then used against the individual who had no knowledge of the information being collected? Currently, many Internet public spaces are being monitored without any notice to forum users or message posters, and therefore without consent.[177] We do not believe it is out of consideration for monitoring or surveillance groups to implement a notice acknowledging at least the possibility of being monitored in a particular chat room or other public space, and we express this recommendation in PAPA.

---

[176] Moira Pascale. "Internet: SEC to start online surveillance system," 1 June 2000, <http://catalogagemag.com/mag/marketing_internet_sec_start/>

[177] ibid

University of Berkeley "Demonstrate" Project

This case study incorporates video surveillance and the power of the Internet. Demonstrate showed how taking video surveillance one step further and broadcasting it on the Internet pushes this video surveillance into the active end of the spectrum. The Demonstrate Project had a surveillance camera broadcasting images online from September 1 through October 15, 2004. From their website,

> "The goal of our[Demonstrate's] installation has been to make people think about privacy in public spaces in conjunction with the 40th Anniversary of the Free Speech Movement at Berkeley"[178]

This project had cameras on the University of Berkeley campus and broadcasted the images online. This illustrated the danger to privacy and anonymity in pervasiveness and distribution of video surveillance over the Internet. Looking through the camera images archive, the images clearly depict specific individuals' actions, and it did not seem the individuals knew they were being videotaped, much less broadcasted over the Internet.

The distribution capability of the Internet, as discussed earlier, makes the surveillance by video cameras placed throughout the University of Berkeley campus even more pervasive and destroys any sense of privacy for the individuals whose actions are being broadcasted online all over the networks. Personal information is collected by cameras, stored and processed into digital information and broadcasted on the networks. There is no human equivalent, because there is no one who can sit there and show everyone what they personally recorded on their own camera. The Internet alone makes this widespread distribution possible. As with video surveillance, there is no opt in/out procedure, and it displays identifiable information.

The Demonstrate project illustrate that many privacy rights are violated when the video surveillance of a public university's public space is broadcasted over the Internet. Demonstrate project recorded Sproul Plaza activity, which was where the roots of the free speech movement of the 1960s took place. There is no consent by the individuals recorded, distribution to unknown third parties, and a lack of privacy protection. This project showed the power of the Internet in eliminating privacy and anonymity of individuals. Recommendations put forth through by PAPA require consent and restrict distribution to ensure the protection of anonymity.

These four examples show the concerns of anonymity in various parts of the identification potential spectrum. The following table is a summary of the analysis framework applied to each of the case studies.

---

[178] Anonymous. <http://demonstrate.berkeley.edu/signin.php>

	Berkeley Demonstrate Project on the Analysis Framework
Human Functional Equivalent	No
Opt-in or Opt-out	No
Pervasiveness	Yes
Personally Identifiable	Yes

Table 11: Summary of Application of Analysis Framework in evaluating anonymity and privacy concerns in Broadcast surveillance through the Berkeley Demonstrate Project.

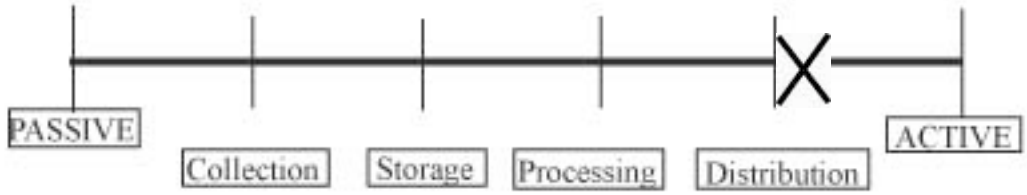

Figure 12: Broadcast surveillance is best placed at the active end of the Spectrum. The threat of pervasiveness in identification is through the distribution of the video images using the Internet as a means of transportation.

Current Legislation

To fully understand the privacy and anonymity issues to date, a legislative background on the Internet is required. We narrowed the scope of the background to information that pertained to privacy, anonymity, monitoring and surveillance legislation and technologies of the Internet.

1974 Privacy Act

The 1974 Privacy Act did not discuss privacy mandates for the Internet, but bring up key points that should be considered when outlining Internet privacy laws. These include:[179]

- Conditions of disclosure. "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains," unless disclosure of the record would be by parties such as government officials or agencies, mandated by court order, or necessary as a statistical research artifact.
- Access to records. "Each agency that maintains a system of records shall (1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system..."

[179] Privacy Act of 1974. <http://www.epic.org/privacy/laws/privacy_act.html>

- Agency requirements. "Each agency that maintains a system of records shall (1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President; (2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs; (3) inform each individual whom it asks to supply information;.. (8) make reasonable efforts to serve notice on an individual when any record is made available to any person under.."

Currently, there is no mandate for disclosure or individual consent and notification for information transmitted over the Internet.

1986 Electronic Communications Privacy Act

The Electronic Communications Privacy Act in 1986 was the first piece of legislation that addressed privacy over electronics. Main definitions include:[180]

I. "electronic communication," which excluded "(B) any wire or oral communication;..(D) any communication from a tracking device as defined in section 3117 of this title.."

II. "readily accessible to the general public," which refers to communication that is not (A) scrambled or encrypted; (B) transmitted using techniques with the intention of preserving the privacy of such communication; ..

III. "electronic storage," pertaining to "(A) any temporary, immediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;…"

Under ECPA it is unlawful to intercept information passed by electronic communication. The main goal of ECPA was largely aimed at preventing invasions of privacy by the government and prohibiting the private sector from divulging information. ECPA particularly looked at surveillance technologies, evaluating the necessity of government surveillance as allowed by the Fourth Amendment. ECPA actually does not control government access to private communications very tightly. In fact, pen registers and trace orders are allowed. There is a great deal of grey area in regards to what is sufficient 'probable cause' to allow surveillance and searches. Now that the Internet has become a dominant means of communication, especially over distant regions, ECPA does not address many new concerns with privacy and anonymity. Our analysis of public spaces on the Internet will look to tighten some definitions and restrictions under ECPA.

2001 USA PATRIOT Act

Under Title II "Enhanced Surveillance Procedures" in the Patriot Act, Congress increased the authority to

---

[180] Electronic Communications Privacy Act (1986). <http://www.usiia.org/legis/ecpa.html>

intercept information along electronic communications, especially for suspicious information relating to terrorism.[181] Congress allowed the government to basically circumvent all privacy issues and use their authority to obtain and disclose any type of information the government found important and essential to national security, with no regard to the sensitivity or privacy of the information. The Patriot Act amended Section 2511117 of Title XVIII in the United States Code with this insertion:

> "(6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived there from, **may disclose such contents to any other** Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence…"[182]

Current legislation allows government officials to be less concerned with protecting individual privacy and anonymity. Additionally, the Patriot Act expanded the information made available to law enforcement officials about subscribers to electronic communication services and allowed government access to location information such as temporarily assigned Internet IP addresses.[183] Lastly, the Patriot Act in Section 217 under Title II made "cybercrime" a federal terrorist offense, thereby allowing the government to intercept electronic communications of intruders to electronic systems without a warrant.[184] This undermines all privacy and anonymity considerations of the individual and the possibility for the government to intercept communication without a warrant does not protect the rights of the individual.

Concerns

As in physical public spaces, the Internet has come under constant surveillance and monitoring. In fact, many believe the Internet is taking the world closer to a "panopticon." Panopticon refers to 18th century philosopher Jeremy Bentham's hypothetical prison where there exists the constant possibility of surveillance by unknown and unseen watchers.[185] Constant surveillance over the Internet point to an increase in use of sensors in the cyberspace world. From an online credit card transaction to an email to a simple mouse-click, personal information is not only collected, but broadcasted, compiled, and stored by unknown personnel.[186] With an increasing amount of personal information transferred by sensors, it is important to address privacy and anonymity concerns on the Internet. We look at privacy and anonymity issues on the Internet with examples developed above using the analysis framework and conclude with suggestions for policy recommendations.

---

[181] Patriot Act 2001. Title II, Sec 201-203. <http://news.findlaw.com/cnn/docs/terrorism/patriotact.pdf>
[182] Patriot Act 2001. Title II, Sec 203. <http://news.findlaw.com/cnn/docs/terrorism/patriotact.pdf>
[183] Patriot Act 2001. Title II, Sec 210. <http://news.findlaw.com/cnn/docs/terrorism/patriotact.pdf>
[184] Patriot Act 2001. Title II, Sec 217. <http://news.findlaw.com/cnn/docs/terrorism/patriotact.pdf>
[185] Jeremy Bentham. Panopticon Letters, <http://cartome.org/panopticon2.htm>
[186] Justin Hall. "The Wireless Angels of our Nature." 14 Oct 2002, <http://www.thefeature.com/article?articleid=20508>

Policy Recommendations

In our recommendations, we consider design principles put forth by Professor Morgan from Carnegie Mellon University to preserve anonymity. Many of the suggestions relate to our study of protection of privacy and anonymity in public spaces.

Key suggestions include:[187]

- "When possible, use technologies that preserve the anonymity of the subjects being observed." This is focusing on technology to achieve anonymity protection. While technology plays a strong role in mandating the level of privacy and anonymity protection, it is not the main focus of our discussion of these rights. We leave it to policymakers and legislation to affect a standard for anonymity protection and privacy rights.
- "Avoid unnecessary centralization of information storage and processing." This is crucial and a big part of PAPA. As stated earlier under the *Storage* part of the framework, it is important to keep storage space isolated so that personal information does not get centralized. DoubleClick.com illustrated the implications of a merger between two companies with large quantities of personal information.
- "Minimize the sharing of data and share only to the extent that is required to perform the system's function." Sharing of data across storage spaces (databases) require processing of information. Again, the importance of serving a *function* is illustrated here.
- "Retain data only as long as required for the performance of the function." This eliminates any possibility of accidental processing of information that is clearly not needed (if data is not required for performance of the function, it is "not functionally essential.").

Additional recommendations from the Internet analysis include:

- Provide notice. This can be in terms of a company privacy policy on the website or using the Platform for Privacy Preferences (P3P) specification[188]. P3P mandates allow individuals to have sufficient information to make an informed decision on whether to permit or refuse provision of personal data.
- User Choice. Following notice, we would be able to suggest further protection by allowing for user choice and consent. This is seen in opt-in/opt-out possibilities, access to information through online records or
- Minimization of distribution: do not distribute the information if there is no need. We stress again for necessitating the purpose of distribution of information. The Internet poses great danger because increased pervasiveness and rampant distribution of information over the networks to all parts of the world can create a dangerous, unprivate pot of easily accessible information. With the Internet, it is important to note that information refers to personal information, communication information, broadcast information, and data information.

[187] Morgan.
[188] Clarke, Roger. "Platform for Privacy Preferences: an Overview." 20 May 1998. Australia.

These recommendations proposed by Morgan and supported by our analysis on the Internet can be expanded to include recommendations proposed by other technologies. For PAPA, these recommendations are synthesized with recommendations from other technologies for a unified set of policies.

Conclusion

Overall privacy concerns for the Internet parallel the values that PAPA addresses in regard to general sensors in public spaces. The concerns specifically discussed in regard to the Internet as a public space are: protection of freedoms for individuals, anonymity in history tracking through cookies, monitoring in public behavior spaces, misuse of public information, consent (lack of) in broadcast surveillance, and unchecked distribution of private information over the Internet domain. The concept of an information commons for the Internet space encourages the freedom to assemble. The increasing trend in monitoring of public behavior spaces detracts from the idea of the Internet as a place that elicits public behavior. Cookies that track user history and activity online bring up concerns in the protection of anonymity. For instance, how does the consumer know when they are being tracked? Consumers also do not know what kind of information is being recorded and if there is anything personally identifiable that may threaten the anonymity of the information collected, stored, processed, and even distributed within the business. PAPA must be clear on what information can and cannot be taken using cookies. From the personal example in public records, the ease for identity theft and misuse of public information raises concerns over the protection of private information. PAPA looks into who gets access to this type of information and for what purpose may other parties request such information. In broadcast surveillance, the issue of third party distribution is addressed and prohibited in PAPA. It is important to realize that a secure environment on the Internet is required to keep identification private. So for sites and programs that require personal certificates, privacy is protected. For other sites, where privacy may not be fully protected, anonymity must be protected so that public spaces and public behavior on the Internet may allow users to interact in a secure manner. The cyberspace world, along with the other technologies discussed earlier have shown the privacy and anonymity concerns with sensors in public spaces and the overall policy recommendations that address such concerns are introduced in PAPA.

Public Anonymity Protection Act (PAPA)

SECTION 1: FINDINGS

§1. Whereas

(a) Congress has recognized the right to privacy in educational records (Family Educational Rights and Privacy Act), electronic communications (Electronic Communications Privacy Act), and other sectors of society (1974 & 1980 Privacy Acts, Driver Privacy Protection Act, Video Privacy Protection Act);

(b) the Supreme Court continues to recognize the a reasonable expectation privacy in public spaces (

<http://www.anu.edu.au/people/Roger.Clarke/DV/P3POview.html>

Katz v. US, *Kyllo v. US*, *McIntyre v. Ohio Elections Commission*);

(c) basic Constitutional protections do not disappear with the introduction of new technologies;

(d) sensors that collect, process, store, and distribute identifying personal information about the actions of citizens in public areas have been increasingly used by private companies and government entities;

(e) the collection, retention, or distribution of identifying data magnifies the risk of misuse, exploitation, or other improper disclosure of personal information

(f) individuals may not always consent to the collection of their personal information

(g) privacy protections in public spaces cannot be guaranteed be self-regulation, continued technological innovation, or limited sector-specific legislation;

(h) the Government must protect the security of public spaces;

(i) private entities still retain the liberties and rights granted by the Constitution;

§2. It is resolved that there is a there is a substantial Federal interest in safeguarding the anonymity of individuals from sensors that collect, process, and disseminate personal information about the actions of individuals in public spaces.

SECTION 2: DEFINITIONS

§1. Definitions for the purposes of this Act

(a) the term 'government agency' shall include Federal agencies, state and local departments and offices, officers, employees, special appointments, third-parties working under contract, decree, or agreement, and any other entity recognized by the Congress, receiving Treasury funds, or otherwise acting and serving in the public interest

(b) the term 'private entities' shall include individuals, companies, corporations, partnerships, organizations, institutions, and other entities who do not receive Federal funds or act and serve in the public interest

(c) the term 'personal information' shall include any data that can identify an individual which is otherwise not readily apparent such as name, sex, age, date of birth, race, ethnicity, religion, Social Security number, telephone number, network address, license plate, health status, marital status, sexual orientation, financial status, arrest record, political affiliation, group membership, educational background, fingerprint, retinal pattern, voice characteristics, or other unique, identifiable, non-anonymous data;

(d) the term 'data' shall include both personal information and non-identifiable information

(e) the term 'public space' or 'public medium' shall encompass any physical or electronic area whose intent or function has open access to a large quantities of people, low barriers or controls to entry, or is subject to Constitutional protections for freedom to assemble;

(f) the term 'sensor' shall encompass any technology, process, or system that is capable of identifying, classifying, or otherwise recognizing an individual's personal information;

(g) the term 'privacy' shall encompass the rights to control one's disclosure of personal information, to conduct transactions without identifying oneself, to bar intrusion into one's personal space, to guard

against misuse or misappropriation of one's personal information

(h) the term 'generation' shall include the process of collection, retention, over-processing, and distribution

(i) the term 'collection' shall include any technology, process, or system capable of capturing data

(j) the term 'retention' shall include any technology, process, or system that records or stores data

(k) the term 'over-process' shall include any technology, process, or system that analyzes stored data, creates new information, or is capable of rendering personal information from non-identifiable data by using algorithms, data-mining, or other computational techniques

(l) the term 'distribution' shall include any technology, process, or system that releases, discloses, or transmits data collected from sensors

SECTION 3: PROTECTION OF PUBLIC ANONYMITY FROM GOVERNMENTS

§1. Government agencies

(a) shall not use sensors to collect personal information in a manner that would constitute an invasion of an individual's reasonable expectation of anonymity in a public space;

(b) shall create internal Privacy Auditing Boards to fill the charge of §3.1.a that

i. shall propose policies that define

1. the necessity of collecting and storing personal information
2. the length of time which personal information will be stored
3. the intended use of stored personal information
4. the agencies, officers, and employees who will be parties to the distribution of personal information

ii. shall make said policies open to a period of public feedback and comments

iii. shall release regular public reports testifying to the agency's sensor activities per §3.1.b.i

iv. shall conduct investigations for claims against the agency, officers, or employees arising from §3.1.c and §3.1.d

(c) shall limit its use of sensors to

i. those uses and activities defined in §3.1.b.i

ii. purposes that do not target individuals solely based on race, gender, ethnicity, sexual orientation, disability, or other classification protected by law;

(d) shall establish and publicly release Fair Information Practices specifying

i. notice in the immediate area of sensor use of the

1. agency collecting data,
2. the nature of the data being collected
3. notice of the intended use for collected data

ii. access to stored personal information by providing

1. a mechanism by which the data collector can verify the information,
2. a simple means for contesting inaccurate or incomplete data,
3. the means by which corrections and/or objections can be added to the data its recipients

iii. adequate security protecting data against unauthorized access, use, or disclosure by
1. defining the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data

2. Notwithstanding any other law, it shall be unlawful for a government agency to
(a) collect personal information in excess of that defined as necessary per §3.1.b.i;
(b) store personal information for times longer than defined as necessary per §3.1.b.i;
(c) utilize personal information for uses not defined as necessary per §3.1.b.i;
(d) distribute personal information beyond parties authorized as necessary per §3.1.b.i;
(e) distribute data to employees of private companies, foreign governments or entities, or non-governmental third parties;
(f) utilize sensors in public spaces that do not meet the requirements per §3.1.d

SECTION 4: PROTECTION OF PUBLIC ANONYMITY FROM PRIVATE ENTITIES

§1. Except as provided in sub-section 2, it shall not be illegal for private entities
(a) to collect, store, over-process, or distribute sensor data
(b) provide public or commercial services using sensor data
(c) protect the rights or property of the private entity from fraudulent, abusive, or unlawful activities using sensor data
(d) distribute sensor data to comply with a subpoena or other court order

§2. Private entities shall further be subject to Fair Information Practices and are required to provide
(a) notice in the immediate area of sensor use of the
i. entity collecting data,
ii. the nature of the data being collected,
iii. notice of the intended use for collected data;
(b) access to stored personal information by providing
i. timely and inexpensive access to data and a mechanism by which the data collector can verify the information,
ii. a simple means for contesting inaccurate or incomplete data,
iii. the means by which corrections and/or consumer objections can be added to the data its recipients;
(c) systems allowing individuals to consent or opt-out of the collection of personal information that will be publicly or commercially distributed
(d) adequate security protecting data against unauthorized access, use, or disclosure by defining the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data

§3. Private entities shall be held legally liable for using sensors in public spaces, or data derived therefrom, and any invasion of personal solitude and/or expectation of anonymity by
(e) collecting, storing, processing, and/or distributing data with the intent to identify anonymous individuals
(f) generating, misappropriating, or using unauthorized personal information

(g) failure to abide by the Fair Information Practices of §4.2

§4. Individuals whose privacy has suffered from willful, negligent, or circumstantial misuse of sensors or unfair information practices are wrongful acts.

(a) Individuals may bring suit against an offending private entity to

i. recover damages

ii. gain access to or control of one's personal information

iii. be granted an injunction against the actions of the entity

Discussion of Public Anonymity Protection Act

The Public Anonymity Protection Act (PAPA) addresses many of the concerns and embodies many of the recommendations we have made. PAPA, first and foremost, is a statue that limits the actions of people using sensors. While we cannot imagine the capability of sensor technologies as they evolve, they will invariably feature capabilities having the same deleterious effect in public spaces on an individual's expectation of anonymity. It is in this vein that the language within PAPA avoids lists of technologies (like those found in the Electronic Communications Protection Act) and focuses on functional properties. The injuries sustained by an invasion of privacy are certainly not universal, but the process by which such an invasion occurs can be modeled on our framework.

These emphasis on functional descriptions (generation, collection, retention, over-processing, distribution), rather than technology-specific features (lens, tape, radio, fingerprint), allows PAPA to be applied to the spectrum of sensors, including those described in our framework. Personal information and identification are not wholly separable concepts but there exists information that is not identifying and allows and individual to remain anonymous. Collapsing both of these under the general definition of “data” encompasses all information that a sensor could collect. PAPA attempts to limit the generation (collection, storage, over-processing, and distribution) of data that explicitly identifies individuals as well as data possessing the potential to implicitly to do so.

The structure of PAPA includes a resolution demonstrating the need for enforceable protection of anonymity, definitions outlining essential terms, and the body of the regulation split between “government agencies” and “private entities.” The choice to distinguish these two actors and the regulations placed upon them stems from different expectations on their actions regarding the public interest. Government agencies are recognized by and accountable to publicly elected officials, derive their budget from public funds, and are charged with serving the public interest. Private entities are essentially all other actors whose funds are privately controlled and held and are not compelled to be accountable to or responsible for public interests beyond civic duties. The distinction in actors' motivation to act in the public interest affects their ability to use sensors in public spaces responsibly.

Government agencies are accountable to elected officials who determine the agency's budget. To create an enforceable statue preventing government agencies and their sensors from "[using] sensors to collect personal information in a manner that would constitute an invasion of an individual's expectation of anonymity in a public place"[189], PAPA requires an internal Privacy Auditing Board (PAB)[190]. PAPA makes no stipulations on the membership or interaction of such a Board with the rest of the agency. Certainly different agencies have different missions and goals and PAPA would be out of place to require all agencies to use their sensors in the same way. Rather, the PAB acts to balance the agency's specific mission and its interaction with the public. PAPA requires these PABs to establish specific policies on sensor use and make these policies publicly available for comments and feedback. Other stipulations like the release of regular reports on the agency's Fair Information Practices and investigative power grants the agency increased legitimacy for its sensor use by making it more accountable to the public.

Fair Information Practices are developed from recommendations made by the Federal Trade Commission in 1998[191]. These practices are developed from common themes in American, Canadian, and European studies on privacy[192]. PAPA requires that both government agencies and private entities provide notice, access, and security for data gathered by their sensors. These practices require the collecting actor to publicly reveal the identity, use, and recipients of the data it is collecting on individuals. Private entities, while unregulated in their actions, are bound by an expanded Fair Information Practices requirement including a consent or opt-out scheme. Government agencies are not required to provide a consent practice because such a requirement would be undermine the mission of many agencies. Major agency missions like public safety or national security are wholly at odds with consent where the same monitoring standard needs to be applied equally and constantly. Indeed, if there was a consent principle, the cost to society from criminals and terrorists opting-out of surveillance would greatly outweigh any marginal increase in privacy. In its place, the activities of the Privacy Auditing Board is viewed as a sufficient check on the ability of the government to abuse sensors and invade personal anonymity in critical government functions. PAPA requires Fair Information practices for both government agencies and private entities because by making sensor use and policy more obvious, it increases an individual's awareness of their constant monitoring and instead of trusting the central authority, it grants the power over one's identity to the individual.

PAPA makes a subtle distinction in data and personal information use between government agencies and private entities. Because personal information is identifiable and thus de-anonymizing data, it should be held to more stringent standards than mere data. At the same time, data includes information that has the potential to be processed, analyzed, or distributed and become identifying. PAPA develops different regulations for government agencies and private entities reflecting the difference in personal information

[189] Public Anonymity Protection Act. §3.1.a
[190] Public Anonymity Protection Act. §3.1.b
[191] Federal Trade Commission. "Fair Information Practice Principles," <http://www.ftc.gov/reports/privacy3/fairinfo.htm#Fair%20Information%20Practice%20Principles>

and data and these actors' public interest. The Privacy Auditing Boards are required only to develop policies pertaining to personal information and not data in general. However, the Fair Information Practices of government agencies and private entities apply to all data collected. PAPA, by imposing limits on data collection and generation, attempts to limit the growth of sensor use to only necessary applications in government agencies and private entities.

The government and private actors have different enforcement schemes, again reflecting their different interests. If government agencies act on behalf of the public or in the public interest, the violations of this trust that occur when the government unnecessarily invades an individual's expectation of privacy are more serious than a privacy entity using sensors irresponsibly. PAPA empowers the sensor and monitoring policies established by an agency's Privacy Auditing Board as law. Sensor use by a government agency that is not defined by it its Privacy Auditing Board policy is a criminal act. This contrasts a private entity's enforcement scheme of torts. Torts are civil, not criminal, wrongs that are grounds for a lawsuit. PAPA recognizes that private entities can willfully or negligently use sensors in public spaces to wrongfully invade an individual's expectation of anonymity. Instances of willful or negligent sensor use can include collecting data with the intent to identify anonymous individuals, failing to abide by established Fair Information Practices, or generating unauthorized personal information. PAPA does not attempt to outlaw or regulate every use of private sensors in public spaces, but rather grants individuals legal standing and recourse against irresponsible or negligent data collectors.

PAPA Feedback

As with any piece of proposed legislation, feedback was sought concerning PAPA. We received feedback from a policymaker, a policy-technology professor, and a law enforcement officer. We incorporated some of their suggestions in our final presentation of PAPA. Here is a summary from the feedback on PAPA.

We met with Professor Granger Morgan (Department Head, Engineering and Public Policy, Carnegie Mellon University) early on in our project and he provided interest insights to certain topics. In particular, he brought up the topic of online public records. The discussion centered around these questions:

- Is there a need for them to be online?
- What rights are being threatened with the move of records from city courthouse to the Internet?
- Are these problems avoidable?

These questions are discussed in the case study on online public records. For instance the need to be online and the move came out of technology convenience. We discuss that within our framework under human equivalent and trying to abstract the technology from the purpose of the information. The last question about whether these rights issues with having records online are solvable problems invite a lot of discourse, which we do not go into further detail here. Essentially, a lot of this paper has looked at what

[192] ibid

can we do to minimize such problems. But to avoid everything? Although not impossible, we think it is very hard to have feasible solutions to all these problems.

While he did not review our legislation, he was aware of the types of recommendations we are making. For instance, he agreed that there is a need to protect anonymity in public, and his past research and publications have noted his involvement in these policy concerns. With Professor Morgan, practical issues were a central focus—*how* exactly should such a system or regulation be implemented to enforce such recommendations on privacy and anonymity protection? How and who will be responsible for checking up on potential violators of protection? With each revision of PAPA, a little more practicality in implementation of this piece of legislation comes about, and there is always another way of addressing the problem.

Elaine Newton (PhD Candidate, Engineering and Public Policy, Carnegie Mellon University) works for Professor Morgan at Carnegie Mellon University. She has worked on many studies in the areas of computer anonymity in design of systems as well as the policy side. She has drafted legislation similar to PAPA before, and we sought her advice and feedback for our own legislation.

There were three main suggestions from Newton:

- narrow the definitions in PAPA. In particular, she looked at these definitions:
    - 'sensor' [Section 2(1)(d)]. This definition is too broad and seems to encompass everything in information technology. Why not keep sensor as the typical interpretation of a sensor—more of a physical entity that is obviously sensing information or change?
      -We debated over redefining 'sensor' in PAPA. However after our analysis over different types of technologies of sensors, it is hard to 'limit' the sensor scope. The world is being watched from all angles, and if some sort of entity is picking up or sensing information, then that entity needs to be included in the 'sensor' definition.
    - 'privacy' [Section 2(1)(e)]. Are we concerned with the actual legal right? Implied right? We should take a closer look and tighten our distinction between identity and property. For instance, the European Union and the United States interpret these two things differently. Newton says she believes the EU considers property as an identity form, while the US does not.
    - 'public space' or 'public medium' [Section 2(1)(c)]. Should pick one or the other, otherwise the definitions are trying to cover everything.
      -Precisely our concern. When formulating PAPA, we want to consider anonymity in public spaces. But spaces is usually termed as physical entities. We cannot, after studying the Internet, limit ourselves to physical domains. Hence, we included 'public medium'.
- look at the practicality of the government entity.

- ‘mission of agency’ [Section 3(1)(a), previous draft which stated “limit the collection to the specific purposes of enforcing and discharging the laws, regulations, and mission of the agency”]. In our final draft of PAPA, we reworded to define what purpose of a sensor is prohibited under the law.

- Is the business section really going to be effective?

  A serious concern, but after evaluating our legal options, we feel tort legislation is one of the better ways to go about enforcing regulations in the private and business sector.

In order to analyze the merits of PAPA, we also obtained feedback from Chief John DiFava of the MIT Police. Before joining MIT law enforcement in December 2001, Chief DiFava was superintendent of the Massachusetts State Police and helped direct security efforts at Logan International Airport after September 11th. Chief DiFava was able to give us valuable commentary from the viewpoint of a law enforcement officer.

Chief DiFava acknowledges the need for federal legislation for video surveillance. He notes that the most important step is for parties to get together and make decisions together. However, any guidelines that are created need to follow the law, and be backed up by the law. Otherwise, guidelines are simply “gentleman’s agreements”. For consistency, he agrees that legislation must be federal, so that there can be no deviations or additions on the state level. As examples of harm created by different state legislation, he raised the examples of the varying legislation between states on usage of the polygraph test and audio recording in video surveillance. He noted that these differences in legislation could make the difference between catching a criminal in one state and letting him or her go due to insufficient evidence in another.

On the specifics set forth by PAPA, Chief DiFava agrees with the restrictions on data collection. He concurs that it is necessary to limit collection, demonstrate the necessity of usage, and that notice should be given. He notes that it is important for law enforcement agencies to maintain credibility in the community, since the police represent a “public service profession.” He acknowledges the need to provide notice of surveillance camera usage, and likens such notice to the search warrant currently needed to collect certain forms of evidence. However, he does state that at times, notice is not necessary, especially when applied to CCTV usage akin to police surveillance, in which law enforcement is looking for specific criminals.

Chief DiFava suggests that legislation relating to storage of information should set a specific limit on the amount of time that data may be kept. He is “uncomfortable with open-ended” guidelines, as they may differ greatly between agencies. He suggests that a study be done to determine the proper length of time for data retention, and notes that public hearings could be helpful in the analysis.

He also had some perspectives on the distribution restrictions set forth in PAPA. He gives the example of

procedures he might follow when trying to track down a missing student. He would want to use the most recent video footage of the student to determine his or her clothing and / or other external effects. The image would then be circulated to as many outlets as possible, including the media and the Internet, to try to track down the student. He notes that PAPA should not prevent such “bona fide law enforcement purposes.”

For law enforcement acquisition of collected images, Chief DiFava notes that the legal system of obtaining court orders is “already tremendously bogged down.” Thus, he argues that if a court order is needed every time that law enforcement necessitates footage collection, the system will be increasingly slowed down. Instead, he suggests that a record, or paper trail be in use whenever video surveillance footage is requested from a private entity. This documentation would need to state the reasons for the requests, to contain approval from the Chief of police, and would establish a “chain of custody” that would denote information such as time of release and the individuals to whom it is released. This system would prevent unauthorized distribution without adding another strain upon the current legal system.

Chief DiFava’s comments were very useful to our development of PAPA. His point about setting a specific time limit upon data storage is well taken. However, because PAPA encompasses so many technologies, it is difficult to cite an exact time limit on the amount of time that data could be stored. Thus, we have recommended that the internal auditing boards of each private agency propose the length of time in which data will be stored, and that this proposal should be made public for commentary and feedback from the community.

PAPA also allows for legitimate law enforcement usage, such as the missing student example cited by Chief DiFava. PAPA is designed to allow each agency to state the necessity of surveillance usage and to note the relevance of these necessities to the mission of the agency. Usage of footage to find missing students is a legitimate objective of law enforcement, and thus would not be prevented by PAPA.

Chief DiFava’s argument against the necessity of a court order for law enforcement usage is also well-argued. We have taken his viewpoint into consideration, so that the private sector is able to release footage to whomever, so long as they provide notice that surveillance images could potentially be distributed to law enforcement agencies. Without proper notice of this possible release, individuals could sue the private entity for damages under PAPA.

It has been valuable to obtain the viewpoint of a law enforcement official in order to consider the real-world applications of PAPA. Although not all of Chief DiFava’s feedback can feasibly be incorporated into PAPA, it is important to note the requirements and commentary of the end-user in order to create an applicable law.

Final Conclusion

The protections contained in PAPA are not the panacea for every potential injury or invasion of one's privacy. While it does attempt to contribute to responsible sensor use by requiring Privacy Auditing Boards and establishing legal grounds for civil cases, these enforcement schemes may only contribute to a negligible decline in the increasing pervasiveness of sensors in public spaces.

Nevertheless, the protections contained within PAPA would address anthropomorphized invasions that happened in the Problem Statement. PAPA would grant you the right to know why your personal information was being collected and for what purpose would it be applied through its Fair Information Practices. It would grant you legal standing to bring a suit to the harassing stalker because he had not given you notice that you were being watched. If it did not prevent the bouncer from giving your information to his cell phone buddy, you would have an equal right to sue him too.

The enforcement mechanisms contained in PAPA are not meant to complicate installation by requiring adherence to Fair Information Practices, increase the size of the bureaucracy through Privacy Auditing Boards, or further aggravate civil litigation through privacy suits, but increase the responsible use of sensors in public spaces. By making them non-obvious, installing them for specific application, and holding their users responsible, we are confident the technology will continue to have a meaningful contribution to society.

Contributions

Keegan, Brian. Introduction. Legal Cases. PAPA. Editor.
Feng, Mabel. Internet. Feedback from Morgan, Newton. Table of Contents, Structural Format.
Chatterjee, Shuvo. RFID. Appendix.
Ma, Sarah. Biometrics. Footnotes and Bibliography.
Wang, Jennifer. Video Surveillance. Feedback from Chief DiFava. Footnotes and Bibliography.

Appendix

PeopleData™

Background Check Results

Scroll Down to See Background Check Report

Background Check
Research Someone from your report

First Name | Last Name | Street Address | City | State (Select State) | Submit

Satellite Photo
See a property from your report

Street Address | City | State (Select State) | Submit

Get Unlimited Background Checks $20 each

IMPORTANT! The National Criminal Record Search will be available by the next business day. You will be notified by e-mail when when the results are available.

126 Sumner St newton MA
Latitude: 42.333831 Longitude: -71.191544

Comprehensive Report

Date: 11/14/2004

Subject Information

HAROLD ABELSON **DOB:** 07/26/1947 **Age:** 57

Most Likely Current Address(es):

126 SUMNER ST, NEWTON CENTER, MA 02459

Previous Address(es):

801 CHURCH ST, MOUNTAIN VIEW, CA 94041

First reported: 12/1995

126 SUMNER ST, NEWTON, MA 02159

First reported: 10/1992

ABELSON, HAROLD 332-3793

126 SUMMER ST, BOSTON, MA 02193

First reported: 7/1985

Possible Relatives:

AMANDA ABELSON aka AMANDA ABELSON

Active Address(es):

126 SUMNER ST , NEWTON CENTER , MA 02459

First reported: 3/2002

ABELSON , AMANDA

126 SUMNER ST , NEWTON CENTER , MA 02459

First reported: 12/1999

ABELSON , AMANDA

126 SUMNER ST , NEWTON CENTER , MA 02459

First reported: 12/1999

ABEISON , AMANDA L

126 SUMNER ST , NEWTON CENTER , MA 02459

First reported: 3/2002

ABELSON , AMANDA LYNN

Previous Address(es):

1 BOWDOIN COLLEGE , BRUNSWICK , ME 04011

First reported: 11/2000

ABEISON , AMANDA L

1129 ALA MOANA BLVD , HONOLULU , HI 96814

First reported: 12/1998

ABELSON , AMANDA LYNN

640 S DAHLIA CIR P204 , DENVER , CO 80246

First reported: 7/1998

ABELSON , AMANDA LYNN

Neighbors:

Neighborhood:

76 SUMNER ST, NEWTON CENTER, MA 02459

First reported: 1/2001

MARC Z BRETTLER
MONICA R BRETTLER

BRETTLER, MARC Z (617) 244-4952

83 SUMNER ST, NEWTON CENTER, MA 02459

First reported: 1/2001

ANN P HOCHBERG

HOCHBERG, ANN P (617) 969-6374

83 SUMNER ST, NEWTON CENTER, MA 02459

First reported: 1/2001

HOWARD J WEINSTEIN

WEINSTEIN, HOWARD J (617) 969-6374

83 SUMNER ST, NEWTON CENTER, MA 02459

First reported: 7/2003

HOWARD J WEINSTEIN

WEINSTEIN, HOWARD J (617) 969-6374

84 SUMNER ST, NEWTON CENTER, MA 02459

First reported: 1/2001

ALAN LEVITON
JOAN M LEVITON
JOAN M LEVITON
ROBERTA E LEVITON

LEVITON, ALAN M (617) 965-0016

87 SUMNER ST, NEWTON CENTER, MA 02459

First reported: 3/2004

HERBERT L KLIGER
PHILIP B KLIGER

90 SUMNER ST, NEWTON CENTER, MA 02459

First reported: 1/2001

KAY E ALEXANDER
MARY J ALEXANDER
MICHAEL ALEXANDER
THERESE M ALEXANDER

ALEXANDER, KAY E (617) 244-2173

98 SUMNER ST, NEWTON CENTER, MA 02459

First reported: 1/2001

AARON G FREEMAN
AMANDA B FREEMAN
DAVID L FREEMAN
JOSHUA E FREEMAN

FREEMAN, AARON G (617) 965-1808

99 SUMNER ST, NEWTON CENTER, MA 02459

First reported: 1/2002

SAEED M MOGADAM

MOGADAM, SAEED M (617) 527-8224

99 SUMNER ST, NEWTON CENTER, MA 02459

First reported: 9/2003

SAEED M MOGADAM

MOGADAM, SAEED M (617) 630-9677

99 SUMNER ST, NEWTON CENTER, MA 02459

First reported: 3/2002

AMIR MOGHADAM
BOBBY MOGHADAM
NASRIN Y MOGHADAM
SAEED M MOGHADAM

MOGHADAM, AMIR Y (617) 527-8224

99 SUMNER ST, NEWTON CENTER, MA 02459

First reported: 4/2001

AMIR MOGHADAM
BOBBY MOGHADAM
NASRIN Y MOGHADAM
SAEED M MOGHADAM

MOGHADAM, AMIR Y (617) 630-9677

99 SUMNER ST, NEWTON CENTER, MA 02459

First reported: 9/2003

AMIR MOGHADUM

MOGHADUM, AMIR (617) 527-8224

99 SUMNER ST, NEWTON CENTER, MA 02459

First reported: 9/2003

AMIR MOGHADUM

MOGHADUM, AMIR (617) 630-9677

Neighborhood:

87 SUMNER ST, NEWTON, MA 02159

First reported: 3/1999

HERBERT L KLIGER

KLIGER, HERBERT L (617) 332-2293

140 SUMNER ST, NEWTON, MA 02159

First reported: 3/2003

DAVID RUBIN

RUBIN, DAVID (617) 965-3948

155 SUMNER ST, NEWTON, MA 02459

First reported: 3/1999

EDNA S HAMILTON
STEPHEN P HAMILTON

HAMILTON, EDNA S (617) 969-5752

166 SUMNER ST, NEWTON, MA 02459

First reported: 3/1999

HANK KEARSLEY
HENRY KEARSLEY

KEARSLEY, HANK (617) 964-0328

Neighborhood:

801 CHURCH ST, MOUNTAIN VIEW, CA 94041

First reported: 2/2004

JUKKA ALANEN

ALANEN, JUKKA (650) 237-9046

801 CHURCH ST, MOUNTAIN VIEW, CA 94041

First reported: 6/2000

MASAFUMI AMINO

AMINO, MASAFUMI (650) 969-3436

801 CHURCH ST, MOUNTAIN VIEW, CA 94041

First reported: 2/2003

RANJU S ATWAL

801 CHURCH ST, MOUNTAIN VIEW, CA 94041

First reported: 3/2003

SUNGHWA BAEK-HAN

BAEK-HAN, SUNGHWA (650) 960-6824

801 CHURCH ST, MOUNTAIN VIEW, CA 94041

First reported: 6/2000

KEVAN A BAKER
KEVAN D BAKER

BAKER, KEVAN A (650) 961-7493

801 CHURCH ST, MOUNTAIN VIEW, CA 94041

First reported: 10/2003

JEREMY A BERGFIELD

801 CHURCH ST, MOUNTAIN VIEW, CA 94041

First reported: 2/2002

JUSTIN BIRNBAUM

801 CHURCH ST, MOUNTAIN VIEW, CA 94041

First reported: 6/2000

JEFF BREIDENBACH

BREIDENBACH, JEFF (650) 210-9135

801 CHURCH ST, MOUNTAIN VIEW, CA 94041

First reported: 3/2002

S BRU

BRU, S (650) 210-8326

801 CHURCH ST, MOUNTAIN VIEW, CA 94041

First reported: 3/2003

SARAH BYRNE

BYRNE, SARAH (650) 938-3103

801 CHURCH ST, MOUNTAIN VIEW, CA 94041

First reported: 3/2003

PATEL H CHIRAG

CHIRAG, PATEL H (650) 903-9220

801 CHURCH ST, MOUNTAIN VIEW, CA 94041

First reported: 5/2003

SHIRLEY CHU

CHU, SHIRLEY (650) 961-8506

801 CHURCH ST, MOUNTAIN VIEW, CA 94041

First reported: 2/2002

ERENIA F COOPERSTEIN
HOWARD L COOPERSTEIN
HOWARD J COOPERSTEIN
SHARI N COOPERSTEIN
SHARI N COOPERSTEIN

COOPERSTEIN, ERENIA F (650) 625-9040

801 CHURCH ST, MOUNTAIN VIEW, CA 94041

First reported: 10/2003

DAVID CROSS

CROSS, DAVID (650) 964-1517

Ownership Information for Historical and Current Addresses

Property

Site Address: 126 SUMNER ST , NEWTON , MA 02459-1957

County: MIDDLESEX

Name Owner 1: ABELSON, HAROLD

Name Owner 2: ABELSON, LYNN

Owners Address: 126 SUMNER ST , NEWTON , MA 02459-1957

Assessed Value: $877,700

801 CHURCH ST, MOUNTAIN VIEW, CA 94041

First reported: 3/2003

PATEL H CHIRAG

CHIRAG, PATEL H (650) 903-9220

801 CHURCH ST, MOUNTAIN VIEW, CA 94041

First reported: 5/2003

SHIRLEY CHU

CHU, SHIRLEY (650) 961-8506

801 CHURCH ST, MOUNTAIN VIEW, CA 94041

First reported: 2/2002

ERENIA F COOPERSTEIN
HOWARD L COOPERSTEIN
HOWARD J COOPERSTEIN
SHARI N COOPERSTEIN
SHARI N COOPERSTEIN

COOPERSTEIN, ERENIA F (650) 625-9040

801 CHURCH ST, MOUNTAIN VIEW, CA 94041

First reported: 10/2003

DAVID CROSS

CROSS, DAVID (650) 964-1517

Ownership Information for Historical and Current Addresses

Property

Site Address: 126 SUMNER ST , NEWTON , MA 02459-1957

County: MIDDLESEX

Name Owner 1: ABELSON, HAROLD

Name Owner 2: ABELSON, LYNN

Owners Address: 126 SUMNER ST , NEWTON , MA 02459-1957

Assessed Value: $877,700

Bibliography

93rd Congress. "Privacy Act of 1974". 31 Dec 1974 <http://www.epic.org/privacy/laws/privacy_act.html>

99th Congress. "Electronic Communications Privacy Act". 5 March 1986. http://www.usiia.org/legis/ecpa.html

104th Congress "Immigration Control and Financial Responsibility Act of 1996," CIS-NO: 96-S523-3, CIS-DATE: April, 1996, SOURCE: Committee on the Judiciary. Senate, DOC-TYPE: Report, DOC-NO: S. Rpt. 104-249, DATE: Apr. 10, 1996, LENGTH: 146 p., SUDOC: Y1.1/5:104-249, CIS/Index, < http://0-web.lexis-nexis.com.luna.wellesley.edu/congcomp/document?_m=84f71f22ec8a491ba40fb00d07edf328&_docnum=1&wchp=dGLbVzb-zSkSA&_md5=3ad74e9d396651b6040e77a93cd95cfc>

107th Congress. "Enhanced Border Security and Visa Entry Reform Act of 2002," Sec.202 (a)(4)(A), < http://0-web.lexis-nexis.com.luna.wellesley.edu/congcomp/document?_m=d00982c906bc226d8daaa2df48afac73&_docnum=5&wchp=dGLbVzb-zSkSA&_md5=ba58ad0f749217a7abf6358228f28ede>

104th Congress. "Personal Responsibility and Work Opportunity Act of 1996," CIS-NO: 96-H271-70, CIS-DATE: December, 1996, SOURCE: Committee on Commerce. House, DOC-TYPE: Hearing , DATE: June 11, 1996, LENGTH: iii+96 p., SUDOC: Y4.C73/8:104-102, CIS/Index, < http://0-web.lexis-nexis.com.luna.wellesley.edu/congcomp/document?_m=c99c5f266641dd42e33ff64fdfcef566&_docnum=2&wchp=dGLbVzb-zSkSA&_md5=620553d938990f553a3fc2cd9ae426af>

107th Congress. "PATRIOT Act". 26 Oct 2001. <http://news.findlaw.com/cnn/docs/terrorism/patriotact.pdf>

ACLU. "ACLU Calls for Public Hearings on Tampa's 'Snooper Bowl' Video Surveillance". Press Release. February 1, 2001. http://www.aclu.org/Privacy/Privacy.cfm?ID=7117&c=130

Alorie, Gilbert and Shim, Richard. "Wal-Mart Cancels 'Smart Shelf' Trial," *CNET News.com*. July 9 2003. http://news.com.com/2100-1019_3-1023934.html?tag=fd_lede1_hed

Anonymous. <http://demonstrate.berkeley.edu/signin.php>

Anonymous. "Biometrics," <http://www.eff.org/Privacy/Surveillance/biometrics/>

Anonymous. "Concern Over Biometric Passports," 30 March 2004, BBC News, http://news.bbc.co.uk/1/hi/technology/3582461.stm

Anonymous. "Digital Identification." <https://digitalid.verisign.com/server/about/aboutFAQ.htm>

Anonymous. "Fair Information Practice Principles," http://www.ftc.gov/reports/privacy3/fairinfo.htm#Fair%20Information%20Practice%20Principles

Anonymous. "Freedom of Information Act Exemptions." <http://www.sec.gov/foia/nfoia.htm>

Anonymous. "Future Library Forum: The New Helsinki Central Library," http://www.aula.cc/projects/futurelibrary/newlibrary.html

Anonymous. "Plugging in, at last." The Economist Technology Quarterly. The Economist, Vol 373, No. 8404. 4 Dec 2004. p. 3-4. XXX "Big Brother." *The Economist*. Dec 2004

Anonymous. "Public Records," 21 May 2003, <http://www.privacilla.org>

Anonymous. "Unfortunately, the Surveillance Superhighway is here. Now!," 28 Oct 2004,

<http://wearcam.org/visualfiltervidescrow.html>

Anonymous. "What is a cookie?" <http://www.webopedia.com/TERM/c/cookie.html>

Applied Digital Systems. http://www.adsx.com

Applied Digital Systems Press Release. http://adsx.com/news/2004/041304.html

Arena, Kelli. "Slain Prosecutor Alone at ATM Before His Death." *CNN.com*, December 10 2003. http://www.cnn.com/2003/LAW/12/09/prosecutor.slaying/index.html

Bentham, Jeremy. Panopticon Letters, <http://cartome.org/panopticon2.htm>

Besser, Howard. "Intellectual Property: The Attach on Public Space in Cyberspace," 28 Oct 2004, UCLA School of Education & Information, <http://www.gseis.ucla.edu/~howard/Papers/pw-public-spaces.html>

Best, Jo. "Zombie RFID Tags May Never Die." *ZDNet*. May 18 2004.

Black, Jane. "Playing Tag With Shoppers' Anonymity." *Business Week.* July 21 2003. http://www.businessweek.com/technology/content/jul2003/tc20030721_8408_tc073.htm

Bolin, Rebecca. "Tracking, Traffic, and Toll Transponders." *Yale LawMeme.* 7 September 2004. http://research.yale.edu/lawmeme/modules.php?name=News&file=article&sid=1606

Bonsor, Kevin. "How E-ZPass Works." *HowStuffWorks*. http://auto.howstuffworks.com/e-zpass.htm

Bonsor, Kevin. "How Facial Recognition Systems Work." *Howstuffworks*. http://people.howstuffworks.com/facial-recognition.htm

Bowman, Erik. "Everything You Need to Know About Biometrics," (Identix Corp., January 2000)

Brain, Marshall. "How WiFi Works," 2004, Howstuffworks, <http://computer.howstuffworks.com/wireless-network3.htm>

Camp, Jean and Y.T. Chien. The Internet as Public Space. 30 Oct 2004, John F. Kennedy School of Government, Harvard University, <http://www.ljean.com/files/spaces.html>

CCTV – Policy and Procedures. Metropolitan Police Department. http://mpdc.dc.gov/info/comm/CCTV_policy.shtm. Accessed 9 December 2004.

Chace, Richard W. *An Overview on the guidelines for Closed Circuit Television (CCTV) for Public Safety and Community Policing*. Security Industry Association. 2000.

Chief DiFava, John. Interview. 17 November 2004.

Clarke, Roger. "A Primer on Internet Technology," V. 15, 19 Feb 1998, Australia, http://www.anu.edu.au/people/Roger.Clarke/II/IPrimer.html

Clarke, Roger. "Platform for Privacy Preferences: an Overview." 20 May 1998. Australia. <http://www.anu.edu.au/people/Roger.Clarke/DV/P3POview.html>

Congressional Research Service. "CRS Report for Congress, U.S. Visitor and Immigrant Status Indicator Technology Program," RL32234, p. 8 < http://www.epic.org/privacy/us-visit/crs_us-visit.pdf>

Criminal Justice Section, American Bar Association. "Electronic Surveillance: Part B: Technologically-Assisted Physical Surveillance" 1999. http://www.abanet.org/crimjust/standards/taps_blk.html

Coughlan, Sean. "Security Under the Skin." *BBC News World Edition*, October 15 2004. http://news.bbc.co.uk/2/hi/uk_news/magazine/3742684.stm

Dennis, Brady. “Ybor Cameras Won’t Seek What they Never Found.” *St. Petersburg Times*. August 20, 2003. http://www.lexisnexis.com/

D'Errico, Richard. "Pataki Announces E-ZPass Privacy Bill." *Business Review*, June 6 2001. http://www.bizjournals.com/albany/stories/2001/06/04/daily36.html

Dewan, Shaila. "30 Narcotics Officers are Shifted in Shake-up Linked to Overtime." *New York Times*, November 17 2003.

Dewan, Shaila K. “Video of Suicide in Bronx Appears on Shock Web Site.” *The New York Times*. April 1, 2004. http://www.lexisnexis.com

Department of Homeland Security. “Docket No. BTS 03-01,”

Department of Homeland Security. “US-VISIT Redress Policy”, http://www.dhs.gov/dhspublic/display?theme=91&content=3776&print=true

DoubleClick.com. <http://www.doubleclick.com>

European Court of Human Rights. *Historical background, Organisation and procedure*. http://www.echr.coe.int/Eng/EDocs/HistoricalBackground.htm. September 2003.

“E-ZPass Account Holder Privacy Statement.” Pennsylvania Turnpike Commission. http://www.paturnpike.com/ezpass/privacy.htm

“E-ZPass Plus.” Port Authority of New York and New Jersey. http://www.panynj.gov/ezpass.html

"Electronic Money." Wikipedia. http://en.wikipedia.org/wiki/Digital_cash

Eng, Paul. "Implant Chip, Track People." *ABC News*, February 25 2004. http://abcnews.go.com/Technology/story?id=98077&page=1

EPCglobal, "How the EPC Network Will Automate the Supply Chain," http://riccistreet.net/port80/charthouse/future/rfid.htm

Feder, Barnaby J. “Technology Strains to Find Menace in the Crowd.” *The New York Times*. May 31, 2004. http://www.lexisnexis.com/

Federal Trade Commission. “Fair Information Practice Principles” <http://www.ftc.gov/reports/privacy3/fairinfo.htm#Fair%20Information%20Practice%20Principles>

FindLaw Constitutional Law Center. *Invasion of Privacy*. http://supreme.lp.findlaw.com/constitution/amendment01/19.html.

Givens, Beth. “Public Records on the Internet: The Privacy Dilemma,” 19 Apr 2002, San Francisco, CA, http://www.cfp2002.org/proceedings/proceedings/givens.pdf

Griswold v. Connecticut, 381 U.S. 479. (1965).

GVS Registry Login. https://gvsregistry.4verichip.com

Garfinkel, Simson. Database Nation. Cambridge: O’Reilly, 2000.

"Gillette Pioneers Breakthrough Technology," *Yahoo Business Wire*, January 6 2003. http://biz.yahoo.com/bw/030106/62365_1.html

Gossett, Sherrie. "Paying For Drinks With Wave of the Hand." *World Net Daily*, April 14 2004. http://worldnetdaily.com/news/article.asp?ARTICLE_ID=38038

Hall, Justin. "The Wireless Angels of our Nature." 14 Oct 2002, <http://www.thefeature.com/article?articleid=20508>

Harris, Gardiner. "Tiny Antennas To Keep Tabs on US Drugs." *New York Times*, November 15 2004. http://www.nytimes.com/2004/11/15/health/15drug.html

Houston Real Time Traffic Map. http://traffic.houstontranstar.org

Howlett, Debbie. "Motorists Can Keep On Rolling Soon." *USA Today*, May 25 2004. http://www.usatoday.com/news/nation/2004-05-25-toll-system_x.htm

"Identification Friend or Foe." Wikipedia. http://en.wikipedia.org/wiki/Identification_friend_or_foe

Johnston, David. "Terror Data to be shared at New Center Near Albany." The New York Times. May 25, 2004. http://www.lexisnexis.com/

Katz v. United States, 389 US 347 (1967).

Kayden, Jerold and Andrew Shapiro. "Is Public Space Dead?," Fall 1999, <http://www.vanalen.org/forums/public_space.htm>

Kyllo v. United States, 533 US 27 (2001).

Law.com Law Dictionary..*Priviliged communication*. http://dictionary.law.com/default2.asp?selected=1615&bold.

Legal Information Institute. Cornell Univeristy. *Law about... right of privacy*. http://www.law.cornell.edu/topics/privacy.html

Legal Information Institute. Cornell University. *Law about... right of privacy: personal autonomy.* http://www.law.cornell.edu/topics/personal_autonomy.html.

"Leo Theremin." Wikipedia. http://en.wikipedia.org/wiki/Leon_Theremin

Macavinta, Courtney. "Privacy advocates rally against DoubleClick-Abacus merger," 22 Nov 1999, CNET News, http://news.com.com/Privacy+advocates+rally+against+DoubleClick-Abacus+merger/2100-1023_3-233413.html

Massachusetts G.L. c. 81A, Section 10. http://www.mass.gov/legis/laws/mgl/81a-10.htm

McCarthy, Anna. *Closed Circuit Television*. The Museum of Broadcast Communications. http://www.museum.tv/archives/etv/C/htmlC/closedcircui/closedcircui.htm

"McDonald's Testing E-Payment System." *USA Today*, May 29 2001. http://www.usatoday.com/tech/news/2001-05-29-mcdonalds-e-payments.htm

McElhenny, John. "Smile, you're on security camera." *The Boston Globe*. March 28, 2004. http://www.lexisnexis.com/

McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995).

Mena, Jesus. "Homeland Security as Catalyst." *Intelligent Enterprise*. July 2004. http://www.intelligenteai.com/showArticle.jhtml?articleID=22102265

Messing, Philip, and Weiss, Murray. "Top Cops Eye Video Villains." *The New York Post*. June 8, 2004. http://www.lexisnexis.com/

mobileCloak. http://www.mobilecloak.com/mobilecloak/index.html

Morgan, Laura W. "Strengthening the Lock on the Bedroom Door: The Case Against Access to Divorce Records Online," Journal of the American Academy of Matrimonial Lawyers, Vol 17:1, 2002, p. 64.

Morgan, M. Granger and Elaine Newton. "Protecting Public Anonymity," *Issues in Science and Technology*, Fall 2004, p. 83-90.

Nader v. General Motors Corporation, 25 N.Y.2d 560 (1970).

New York City Surveillance Camera Project. Project Information. http://www.mediaeater.com/cameras/breakdown.html

Nieto, Marcus, Johnston-Dodds, Kimberly, and Simmons Charlene. "Public and Private Applications of Video surveillance and Biometric Technologies." California Research Bureau. March 2002.

Olmstead v. United States, 277 U.S. 438 (1928).

"Part 1: Active and Passive RFID: Two Distinct, But Complementary, Technologies for Real-Time Supply Chain Visibility." Auto-ID Center. http://www.autoid.org/2002_Documents/sc31_wg4/docs_501-520/520_18000-7_WhitePaper.pdf

Pascale, Moira. "Internet: SEC to start online surveillance system," 1 June 2000, <http://catalogagemag.com/mag/marketing_internet_sec_start/>

Peck v. United Kingdom. The European Court of Human Rights (Fourth Section). Strasbourg. 28 January 2003.

Phillips, P. Jonathon, Martin, Alvin, Wilson, CL, Przybocki, Mark. National Institute of Standards and Technology. "An Introduction to Evaluating Biometric Systems." IEEE. February 2000.

Privacilla, <http://www.privacilla.org>

Ranalli, Ralph, and Klein, Rick. "Surveillance targeted to convention." *The Boston Globe*. July 18, 2004. http://www.lexisnexis.com/

Reno v. Condon, 528 U.S. 141 (2000).

"RFID." Wikipedia. http://en.wikipedia.org/wiki/RFID

Rheingold, Howard. "Helsinki's Aula," 17 July 2002, <http://www.thefeature.com/article?articleid=15435&ref=4529009>

Roberts, Paul. "VeriSign to Manage RFID 'Root' Server." The Industry Standard, 13 January 2004. http://www.thestandard.com/article.php?story=20040113174055565

Robinson, Brian. "NIST Puts Fingerprints To The Test," July 19, 2004, Federal Computer Week, http://www.fcw.com/fcw/articles/2004/0719/tec-fingerprint-07-19-04.asp

SecurityFocus. "Verisign's SiteFinder Finds Privacy Hullabaloo." *The Register*, September 19 2003. http://www.theregister.co.uk/2003/09/19/verisigns_sitefinder_finds_privacy_hullabaloo/

Shannon, Elaine. "Big Brother Inc.," 29 March 2004, Time Magazine, http://www.time.com/time/insidebiz/article/0,9171,1101040405-605473,00.html

SIRIT Technologies. http://www.sirit.com

Slevin, Peter. “Police Video Cameras Taped Football Fans.” *The Washington Post*, February 1, 2001. http://www.lexisnexis.com/

Spielman, Fran and Main, Frank. “City Plans Camera Surveillance Web”, *The Chicago Sun-Times*. September 10, 2004. http://www.lexisnexis.com/

Staedter, Tracy. “Iris Identification: How The Technology Behind Biometric Security Works,” March 2003, MIT Technology Review, http://www.technologyreview.com/articles/03/03/visualize0303.asp?p=1

Stanley, Jay and Steinhardt, Barry. “Drawing a Blank: the failure of facial recognition technology in Tampa, Florida.” *An ACLU Special Report*. January 3, 2002.

State of California. “Online Privacy Protection Act of 2003 (OPPA)”, California Business and Professions Code § 22575-22579. http://www.leginfo.ca.gov

“State Police, PCCD Announce Changes to Improve Collection, Sharing of Information by Law Enforcement Agencies.” Pennsylvania State Police Press Releases. August 27, 2003. http://www.psp.state.pa.us/psp/cwp/view.asp?A=11&Q=170383

Sweeney, Latanya. “k-Anonymity: A Model for Protecting Privacy.”, May 2002, Carnegie Mellon University, <http://privacy.cs.cmu.edu/people/sweeney/kanonymity.pdf>

"Technology Helps Commuters Avoid Congestion." Texas Transportation Institute: Return on Research. http://tti.tamu.edu/product/ror/congestion.pdf

“Terror-fighting network touted.” *The Washington Times*. February 25, 2004. http://www.lexisnexis.com/

"Tracking Junior With a Microchip." *Wired News*, October 10 2003. http://www.wired.com/news/technology/0,1282,60771,00.html

Trigaux, Robert. “Cameras Scanned Fans for Criminals.” *St. Petersburg Times*, Jan 31, 2001. http://www.lexisnexis.com/

“Troopers to be hands-off with Tuscaloosa traffic cameras”. *Associated Press*. January 15, 2004. http://www.lexisnexis.com/

United Nations, Universal Declaration of Human Rights, G.A. Res. 217A(III), U.N. GAOR, 3d Sess., U.N. Doc. A/810 (1948), art. 12, reprinted in M.Rotenberg Ed., The Privacy Law Sourcebook 2003 318 (EPIC 2003)

United States Department of Justice Criminal Resource Manual No. 32, Title 9-618. “Video Surveillance – Use of Closed-Circuit Television (CCTV)”.

United States District Court for the Northern District of California. “Gilmore v. Ashcroft,” No. C 02-3444 SI. http://0-web.lexis-nexis.com.luna.wellesley.edu/universe/document?_m=b86a410217033450956a0955bd4a8344&_docnum=2&wchp=dGLbVzb-zSkVb&_md5=af003ba250f11fa8668b1c9ae64e7146

United States Supreme Court. “Janet Reno v. Bill Pryor,” No. 99-61. http://www.usdoj.gov/osg/briefs/1999/2pet/7pet/99-0061.pet.aa.html

"VDOT'S Smart Tag - Protecting Patron Privacy." Virginia Department of Transportation Privacy Policy. https://smart-tag.com/privacy.cfm

“VeriChip,” Wikipedia. http://en.wikipedia.org/wiki/Verichip

VeriChip. http://www.4verichip.com

Vo v. City of Garden Grove, 115 Cal.App. 4th 425, 2004 Cal. App. Lexis 116.

Wallack, Todd. "They Know where You've Been: Data Collected From FasTrak Drivers Raise Privacy Concerns." *San Francisco Chronicle*, 12 February 2001. http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2001/02/12/BU75523.DTL

Warren, Samuel. Brandeis, Louis. *Right to Privacy.* Harvard Law Review 4, no. 5 (1890).

Weiss, Murray. "Suicide Video Shock – Linked to L.I. Cop". *The New York Post*. April 6, 2004. http://www.lexisnexis.com

White, James C. "People, not Places," Spring 2003

Woodward Jr., John D. "Super Bowl Surveillance: Facing Up to Biometrics," 2001, RAND, <http://www.rand.org/publications/IP/IP209/IP209.pdf>

Yoshida, Junko Yoshida. "RFID Backlash Prompts 'Kill' Feature." *EETimes*. April 28 2003.