INSTITUTO TECNOLOGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS MONTERREY

ESCUELA DE GRADUADOS EN ADMINISTRACION PUBLICA Y POLITICA PUBLICA

TECNOLÓGICO DE MONTERREY

Revisiting the Development of Privacy and Future Implications

Tesina

POR:

James D. Newsom

MONTERREY, N. L. MAYO DE 2008

INSTITUTO TECNOLOGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY
CAMPUS MONTERREY
ESCUELA DE GRADUADOS EN ADMINISTRACION PUBLICA Y POLITICA PUBLICA

TECNOLÓGICO DE MONTERREY

Revisiting the Development of Privacy and Future Implications

Tesina

Por

James D. Newsom

Monterrey, Nuevo León Mayo de 2008

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY
Campus Monterrey

ESCUELA DE GRADUADOS EN ADMINISTRACIÓN PÚBLICA Y POLÍTICA PÚBLICA

Revisiting the Development of Privacy and Future Implications

Tesina

Por
James D. Newsom

Monterrey, Nuevo León Mayo de 2008

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY
Campus Monterrey

ESCUELA DE GRADUADOS EN ADMINISTRACIÓN PÚBLICA Y POLÍTICA PÚBLICA

Los miembros del comité de tesina recomendamos que el presente proyecto de tesina presentado por James D. Newsom sea aceptado como requisito parcial para obtener el grado académico de:

Maestro en Derecho Internacional

Comité de Tesina:

Dr. Roberto Garza Barbosa
Asesor

Dr. Gabriel Cavazos Villanueva
Sinodal

Lic. Noé Galván Martínez
Sinodal

Dra. Teresa Almaguer Salazar
Directora Académica de la EGAP
Mayo 2008

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY
Campus Monterrey

ESCUELA DE GRADUADOS EN ADMINISTRACIÓN PÚBLICA Y POLÍTICA PÚBLICA

Revisiting the Development of Privacy and Future Implications

by
James D. Newsom

SUMMARY:

Privacy is a concept that is relative and subjective to numerous factors including time, culture, tradition, religion, economic well-being, and the situations in which it is invoked. Its sensitivity to these factors causes it to constantly evolve and respond to changes in societal structures as new norms are adopted and advances in technologies are incorporated into daily life. ... The U.S. and European privacy regimes have developed and evolved in separate directions and thus value and enact legal privacy protections differently, each seeking to balance the competing values that privacy influences. The U.S. model has been largely a sectoral, *ad hoc* approach, whereas the European model stresses the fundamental nature of privacy rights and enforces them from the top down in an *omnibus* fashion. ... Most of the international disputes over privacy involve the sharing, distribution, and dissemination of personal data, but there are other concerns that transcend national borders as governments are increasingly utilizing new tools to spy on their citizens and those of other countries in the name of national security and anti-terrorism. ...

HIGHLIGHT:

Privacy is once again in the forefront of political and societal debate as new technologies and security concerns threaten the balance of privacy rights. This article examines the conceptual and philosophical bases of privacy and the legal structures of the two dominating privacy regimes currently vying for power in the international arena – the United States and Europe. A further exploration of new threats to individual privacy will illustrate the need for increased awareness of the issues and open deliberation in solving the dilemmas of modern privacy vis-à-vis other competing societal aims.

TABLE OF CONTENTS

"Privacy is integral to freedom. You cannot have a free and democratic society without privacy. When a state morphs from a democracy into a totalitarian regime, the first thread to unravel is privacy."[1]

[1] Ann Cavoukian, Information and Privacy Commissioner, Ontario, Canada, Address at the University of Waterloo Computer Science Club: "Privacy by Design": A Crucial Design Principle (Feb. 27, 2007) (video available at http://csclub.uwaterloo.ca/media/Privacy%20by%20Design.html).

I. Introduction

Privacy rights have been a relevant and much debated theme through out modern times. Much of this debate has been fueled by new technologies and changing perceptions of their use and inclusion into everyday life. Now more than ever privacy is back in the forefront of political and legal discourse as societies and governments are forced to deal with new intrusive technologies and threats. Society's quest to determine the proper balance between the individual's right to privacy and the public's right to know continues to be elusive. In the one hundred plus years of debate no conclusion has been reached, nor has this balance been reached. Now that governments all over the world have a mandate to protect society from terrorism and national security concerns there is an increased erosion of privacy rights in exchange for public safety, but does this exchange have to be a zero-sum solution? In other words, can a balance be reached to preserve privacy rights and provide the public with a reasonable amount of security in light of the September 11th and other attacks worldwide?

The globalization and greater unification of the world in conjunction with new, powerful technologies and national security threats has put into doubt expectations of privacy. In the post 9/11 era the emphasis on national security and sophisticated information networks are creating new challenges in preserving everyday and fundamental privacy rights.

Public and private institutions, often in collusion, are rapidly adopting new technologies to quietly and often obtrusively intrude into almost every aspect of life. Big Brother as described in George Orwell's *1984* is no longer fictional idea, but quickly becoming a reality: "It was even conceivable that [the Though Police] watched everybody all the time...every sound you made was overheard, and, except in darkness, every movement scrutinized."[2] Governments worldwide in the interest of public safety and security are creating new, powerful surveillance societies that unlike the Though Police in *1984* are developing the means to watch your every move. Further, Orwell seemed omniscient in many aspects of today's surveillance society, but even he could not predict the maturing

[2] GEORGE ORWELL, *1984* 3 (Signet Classic 1961) (1949).

technologies such as RFID chips, brain scans, facial recognition cameras, biometrics, and information networks that are quickly and pervasively being utilized unchecked and unregulated by public and private institutions. Technologies are not just eroding privacy, but forcing us to rethink what privacy means. Unless new concepts of privacy are universally adopted to confront these developing technologies, a dim future in respect to privacy rights is likely.

Recent remarks made by the Deputy Director of U.S. Intelligence Donald Kerr raise new questions as to how the U.S. Government perceives privacy. He indicated that Americans should change the way they view privacy and instead be confident that government and private institutions will be benevolent guardians of the intimate details of their lives. Kerr said that "privacy, I would offer, is a system of laws, rules, and customs with an infrastructure of Inspectors General, oversight committees, and privacy boards on which our intelligence community commitment is based and measured. And it is that framework that we need to grow and nourish and adjust as our cultures change."[3] This attempt to redefine privacy is disturbing as news reports surface daily concerning both government and private sector data breaches of personal information. It is unsettling that the alternative being pushed upon us is to blindly trust these institutions that have a history of ineptness, abuse, and priorities that do not always coincide with or value privacy as an institution.

Information technology is radically changing and improving. Google's bid to purchase Doubleclick[4] and Microsoft's recent bid to purchase Yahoo![5] signal a market shift that will create powerful, consolidated information clearinghouses that have great potential to

---

[3] Donald Kerr, Principal Deputy Director of National Intelligence, Remarks and Q&A at the 2007 GEOINT Symposium (Oct. 23, 2007) (transcript available at http://www.dni.gov/speeches/20071023_speech.pdf).

[4] Google's merger with DoubleClick raises serious concerns that Google will be able to collect massive amounts of personal data. Jeffery Chester of the Center for Digital Democracy notes that "Google will be able to develop the most detailed profile of users from around the world" and "it will become the world's private ministry of information." *See* Catherine Rampell & Frank Ahrens, *Google's Ad Reach My Be Unrivaled; FTC Approves DoubleClick Deal*, WASH. POST, Dec. 21, 2007, at D1.

[5] Like the Google/DoubleClick merger, the same privacy concerns are raised with Microsoft's bid for Yahoo!. *See* Miguel Helft & Andrew Ross Sorkin, *Eyes on Google, Microsoft Bids $44 Billion for Yahoo*, N.Y. TIMES, Feb. 2, 2008, at A1. Like the Google/DoubleClick merger, the same privacy concerns are raised with Microsoft's bid for Yahoo!.

impact not just privacy rights, but personal freedom. Yahoo!'s participation in divulging private information on Chinese political dissidents to the Chinese government is a prime example of the impact a company like Yahoo! can have over an individual's life.[6] During U.S. Congressional testimony concerning Yahoo!'s involvement Congressman Tom Lantos commented that "while technologically and financially you [Yahoo!] are giants, morally you are pygmies."[7] This is the crux of the problem, Yahoo!'s priorities in seeking out new market penetration and protecting its bottom line do not coincide with an individual's right to privacy. The question is, as a society, can we trust a government or corporation to protect our interests in controlling personal information?

Is there a fundamental right to privacy? What are our privacy expectations and how does one balance these expectations within the current contexts of stopping international terrorism and protecting national interests and everyday security? How can advances in technologies and aggressive government and private spying be regulated to protect an individual's right to privacy?

The former CEO of Sun Microsystems, Scott McNealy, was quoted saying that "privacy is dead, get over it."[8] The bluntness and negativity of McNealy's comment is stirring, but privacy is still viable, only to be, once again, confronted with new challenges. There *is* a fundamental human right to privacy, but this right is largely misunderstood, quixotic, and highly susceptible to restraint (both in the historical and current contexts) when technology, politics, law, and freedoms of expression collide. Tension between public and private information is at an all time high as privacy rights are eroding so that a superficial level of security is achieved.

The scope of this work will be to discuss how emerging technologies and the global focus on national security have created new challenges to preserving privacy rights. The adoption of these powerful technologies has been accelerated as the security-privacy

---

[6] *See* Wang Xiaoning v. Yahoo!, No. 07-2151 (N.D. Cal. Apr. 19, 2007) (complaint of tort damage). In the complaint, Yahoo! is accused, among other things, of voluntarily providing private information to Chinese officials resulting in the imprisonment of political dissidents.
[7] Catherine Rampell, *Yahoo Lied About China, Legislators Say*, WASH. POST, Nov. 7, 2007, at D5.
[8] *On the Record: Scott McNealy*, S. F. CHRON., Sept. 14, 2003.

pendulum has made a large shift towards the side of security often without regard to the consequences of lost liberties. Part II of this work will discuss the concept of privacy (its philosophical origins). Understanding the philosophical roots behind privacy is an important step in fully appreciating the importance of privacy rights in the legal context. Part III is an introduction of how the two dominant privacy regimes apply very different concepts of privacy into their legally systems. It will first examine the development of privacy in the U.S. constitutional and statutory laws. The U.S. legal framework will then be juxtaposed with the development of the European concept of privacy as a fundamental human right through the prominent privacy treaties and directives. Lastly, Part IV will describe up-and-coming technologies and security initiatives that are beginning to have significant impacts on privacy. The discussion of government and private espionage, data mining, biometrics, RFID chips, brain scanning, and other technologies will illustrate the need for increased awareness of privacy issues and open deliberation in solving the dilemmas of modern privacy vis-à-vis other competing societal aims.

II. Defining Privacy

What is privacy? This simple question has been the source of constant debate, consternation, and disaccord. Attempting to answer this question is further complicated as it invariably raises other intertwined and inseparable questions such as: What does privacy entail and protect?; Is privacy a right or merely an interest worth protecting?; and Why is privacy so hard to define? Privacy is a concept that is relative and subjective to numerous factors including time, culture, tradition, religion, economic well-being, and the situations in which it is invoked. Its sensitivity to these factors causes it to constantly evolve and respond to changes in societal structures as new norms are adopted and advances in technologies are incorporated into daily life. Further, privacy's transcendental nature does not allow it to be "fixed" into single categories or thoughts – there is not a single definition that can encompass all of the complicated interests that form the right to privacy, but perhaps instead it should be merely accepted as something of value worth protecting.

The word privacy has its roots from the classic Latin word prīvātus meaning to be "set apart, belonging to oneself."[9] This early definition merely gave differentiation to things that were not public. Today, this public-private divide is still an important part of the definition of privacy, but only part of the whole meaning. Black's Law Dictionary defines privacy as "the condition or state of being free from public attention to intrusion into or interference with one's acts or decisions" and provides two sub-definitions:

1) *Autonomy privacy*: The individual's right to control his personal activities without outside interference, observation, or intrusion.
2) *Informational privacy*: A private person's right to choose to determine whether, how, and to what extent information about oneself is communicated to others.[10]

Dictionary definitions may seem to be the logical starting place when trying to determine the meaning of a word or concept, but in this case it makes little sense. Dictionaries are inherently limited, they provide a basic illustration, but leave the inquisitor lacking the relevant background to fully understand a words meaning. Philosophers, lawyers,

[9] THE OXFORD ENGLISH DICTIONARY, VOL. VIII 1388 (1978 ed.).
[10] BLACK'S LAW DICTIONARY 1233 (8th ed. 2004).

psychologists, and theologians have written thousands of pages trying to determine the meaning of privacy, it is unreasonable to assume that it can be solely encompassed in a few lines of a dictionary.

Perhaps the most renowned definition of privacy is "the right to be left alone,"[11] introduced in a Harvard Law Review article by two aspiring lawyers Samuel Warren and Louis Brandeis. For Warren and Brandeis, this conceptualization of privacy was as a result of the advances of camera technology and the unauthorized publication of photographs. They argued that privacy should be regulated through tort law to afford protection to the violation of an individual's privacy. Even though this definition is over 100 years old it is still one that has a high degree of validity due to the fact that it has been applied to counter many of the societal and technological impacts to privacy over the past century. The "right to be left alone" was just as easily invoked in 1890 to combat nosy photographers as it is today to counter the many intrusions into an individual's privacy. But given the technological advances since 1890, Warren and Brandeis could not have imagined, nor intended, that their "right to be left alone" would be used in cases ranging from abortion to aerial surveillance, and for this reason it is becoming progressively more difficult to invoke this definition in the modern sense of the meaning of privacy.

Its definition is too general, vague, and misleading to account for the important concepts that modern privacy entails. For example, it would be accepted that the right to be left alone is paramount to the freedom an individual has from an overbearing government or private sector intrusion into one's personal affairs, but can this "right to be left alone" be invoked to argue that it is improper to gossip about publicly available personal information? Would casually peering into someone's shopping cart at the grocery store be violating the right to be left alone? Lastly, does a company like Amazon.com violate a person's right to be left alone by using past purchase data to suggest other books the purchaser might be interested in? Certainly the latter examples may irritate one's boundaries of private space and the decorum of appropriate behavior, but it can hardly be

[11] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

used in defense of privacy in relation to the right to be left alone. For this reason it is essential to look deeper into the varying theories as to what exactly privacy entails.

A. Privacy in the Context of Intimacy

Charles Fried in his 1968 article, *Privacy*, contextualizes the right to privacy by equating it as a necessary part of human relationships. Thus, he affirms that "without [privacy] one cannot fully develop friendship, love and trust."[12] He argues that the act of entering into relationship entails different degrees of intimacy that through privacy one controls the sharing of private information such as beliefs and emotions. Mutual respect of the other's privacy forms the "moral capital" that in turn enables the parties to create an atmosphere of love and friendship.[13] Privacy in its complete sense not only allows us to "define our relations to others but also to our freedom to define ourselves."[14] If one's actions and mistakes were constantly monitored or scrutinized without the intimacy to determine the extent of one's relations or the ability to retract into solitude, then one cannot completely and independently develop individual thought processes, beliefs, values, or consciousness. In sum, Fried in his reasoning seeks to show the importance of privacy as related to our basic values of intimacy and the symbiosis to individual development and interpersonal relationships.

Not all philosophers agree with Fried's view of intimacy. Jeffrey Reiman refutes the withholding of information in the context of intimacy in relationships with his theory that "privacy is a social ritual by means of which an individual's moral title to his existence is conferred."[15] In Reiman's opinion, the true essence of relationships is the act of caring and the sharing of experiences, not just "swapping information." He offers the example of someone divulging intimate secrets to a psychologist. The revelation of information does not imply that the psychologist and the patient have necessarily formed an intimate relationship or love. Instead, the sharing of information and the lessening of privacy only

---

[12] Charles Fried, *Privacy*, 77 YALE L.J. 475, 477 (1968).
[13] *See id.* at 484.
[14] *Id.* at 485.
[15] Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, 6 PHILOSOPHY AND PUBLIC AFFAIRS 26, 39 (1976).

furthers one's desire to care and be intimate.[16] In his words privacy is "a right which protects [the] capacity to enter into intimate relationships, not because it protects [the] reserve of generally withheld information, but because it enables [one] to make the commitment that underlies caring."[17]

B. Privacy as personal autonomy

Intrusion, surveillance, and control of personal information are often entered into the privacy debate as inhibitors to an individual's personal autonomy and self-determination. The argument is that one's autonomy is essential to the creation of one's self or "personhood" and everyone should have the right to develop without the interference of intrusion. Reiman defines this condition as the ownership of an individual's "physical and mental reality in the sense that he is morally entitled to realize his destiny through it, and thus that he has at least a strong presumptive moral right not to have others interfere with his self-determination."[18]

It is important to note that human beings are social creatures that do not live in isolation. The very nature of being human involves the interaction with others, therefore privacy in its perfect sense (*e.g.*, complete seclusion) is impossible. Having understood this, the next question is, to what degree of isolation or privacy should one have within the context of society? Stanley Benn promotes that the "general principle of privacy might be grounded on the more general principle of respect for persons."[19] He argues that interaction with others, whether it be in close personal relationships or as a private citizen, is intrinsically tied to a basic, mutual respect. Through this mutual respect individuals are allowed to achieve a high degree of autonomy and personal choice. Christopher Bryant furthers this argument seeing that privacy should focus on "the capacity of the individual to manage the presentation of his self to others,"[20] even though this autonomy of choice may at times be paradoxical within the contexts of social interaction. He illustrates this point by

---

[16] *See id.* at 33-34.
[17] *Id.* at 44.
[18] *Id.* at 39.
[19] Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 228 (Ferdinand D. Schoeman ed., 1984).
[20] Christopher G.A. Bryant, *Privacy, Privatisation and Self-determination*, in PRIVACY 67 (John B. Young ed., 1978).

questioning the woman who is offended at the thought of a peeping tom watching her undress, but who will freely choose to sunbathe topless.[21] Privacy need not resolve these contradictions of social interaction because it forms the basis of self identity and expression, what is important is that one has the choice to be private or public based on his individual notions of acceptability.

Proponents of the necessity of autonomy see surveillance and observation (especially by the state) as the antithesis and the most serious threat to autonomy. Alan Westin worries that forced intrusion into one's "psychological armor" will subjugate the person's most inner secrets to others, thus loosing a certain amount of personal control and individual sovereignty.[22] Kent Greenawalt remarks that:

> A substantial degree of freedom from observation is essential if there is to be any genuine autonomy; and real choice also depends on the ability of persons to enjoy states of privacy without intrusion. Thus, control of and freedom from intrusion are, in part, means by which greater autonomy exists.[23]

For these reasons the proponents often distinguish privacy as an integral part of free, democratic societies invoking such ideals as liberty. John Locke discusses man's entering into a social contract to form a government. The act of creating the contract assumes that a certain amount of freedom and autonomy is ceded to the government in exchange for peace and security.[24] But entering into the contract did not mean one lost all liberty, according to Locke, the contract's ultimate goal is to preserve liberty.[25] Similarly, J.S. Mills in his memorable essay, *On Liberty*, critiques government control and tyranny of its citizens and characterizes liberty as the "inward domain of consciousness; demanding liberty of conscience, in the most comprehensive sense; liberty of thought and feeling; absolute freedom of opinion and sentiment on all subjects, practical or speculative, scientific, moral, or theological."[26] In 1860, the concept of privacy had not yet been fully

---

[21] See *id.*
[22] Alan F. Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's: Part I: The Current Impact of Surveillance on Privacy*, 66 COL. L. REV. 1003, 1023 (1966).
[23] Kent Greenawalt, *Privacy and its Legal Protections*, THE HASTINGS CENTER STUDIES: THE FUTURE OF INDIVIDUALISM, Sep. 1974, at 49.
[24] JOHN LOCKE, SECOND TREATISE OF GOVERNMENT, § 97 (1690).
[25] *Id.* at § 222.
[26] J.S. MILLS, ON LIBERTY, ch. 1 (1860).

developed, but Mills' sense of liberty clearly infers the necessity of privacy as an important individual function in free societies; liberty and privacy are synonymous in this aspect.

In contrast, privacy in totalitarian societies does not exist as the totalitarian state demands absolute loyalty through destroying individual relationships and free expression by instilling surveillance systems to ensure the hegemony of state. Democratic societies depend on individualism, openness, and innovation to survive. Privacy creates the atmosphere for the cultivation of "sociability, expression of independent ideas, resolution of community conflicts, criticism of government, and formation of a consensus on public policy."[27] Seeing that democratic societies have a strong interest preserving and furthering the basic ideals that make their societies free, privacy must be protected as the basis for autonomy and public participation.

C. Privacy in the information age

Before the advent of the Information Age the quantity of information was restricted to the limits of physical storage space and accessing the information was inefficient, often requiring physical presence. Effectively, there was no real threat to information privacy. Today, the use of computers now allows seemingly unlimited amounts of digital storage space and instantaneous access of vast amounts of personal information prompting scholars to take a new look at privacy. The adoption of these technologies is changing the way people interact with each other and has created new privacy implications as both private and public organizations are able to cheaply and efficiently store vast amounts of personal information. Viktor Mayer-Schönberger contends that information retention is challenging society's capacity to forget: "in our analog past, the default was to discard rather than preserve; today the default is to retain."[28] The ramifications of uninhibited information retention will "constrain our willingness to engage in and further our open

[27] For a further discussion of the differences between totalitarian and democratic societies, see Westin, *supra* note 22, at 1018-20. Also, *see* THE FEDERALIST NOS. 10, 51 (James Madison). The Founding Fathers certainly took the protection of liberty and the benefits of diversity in opinion seriously. Madison in these two papers argues that one of the government's primary functions should be the protection of liberty, which is indispensable to the life of government.

[28] Viktor Mayer-Schönberger, *Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing* 4 (Kennedy Sch. of Gov't, Working Paper No. RWP07-022, 2007).

society."[29] Richard Wasserstrom furthers this idea by arguing that "an inevitable consequence of such a practice of data collection would be that persons would think more carefully before they did things that would become part of the record. Life would to this degree become less spontaneous and more measured."[30]

Information technology has forced philosophical and legal theorists to update the concept privacy from new angles to resolve the conflicts the technologies have created. Alan Westin's modern definition of privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[31] Since one's wish to have privacy is equally motivating as one's wish for societal participation, the individual is in constant adjustment, balancing the information he wishes to disclose.[32] He maintains that limited communication is the only realistic way to preserve privacy in the complexities of modern and especially urban life.[33]

Fried, like Westin, agrees that control of information is important and offers the view that:

> Privacy, thus, is control over knowledge about oneself. But it is not simply control over the quantity of information abroad; there are modulations in the quality of the knowledge as well. We may not mind that a person knows a general fact about us, and yet feel our privacy invaded if he knows the details. For instance, a casual acquaintance may comfortably know that I am sick, but it would violate my privacy if he knew the nature of the illness. Or a good friend may know what particular illness I am suffering from, but it would violate my privacy if he were actually to witness my suffering from some symptom which he must know is associated with the disease.[34]

His simple example highlights the potential violations that could occur without proper control surrounding the control of information. This is difficult though because not all

---

[29] *Id.* at 23.
[30] Richard A. Wasserstrom, *Privacy: Some Arguments and Assumptions*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 328 (Ferdinand D. Schoeman ed., 1984).
[31] ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).
[32] *Id.*
[33] Westin, *supra* note 22, at 1022.
[34] Fried, *supra* note 12, at 483.

information is sensitive to violations of privacy and depends on the situation or relationship in which it is asked.[35]

Additionally, Judith DeCew notes that information privacy is extremely relative "because what counts as personal information may vary from group to group or individual to individual, and may change over time, there is no fixed realm of the private."[36] Most of the scholars focus their energies and analysis on the types of intimate information that ought to be protected, but Helen Nissenbaum correctly asserts that many non-intimate forms of information could have a substantial chilling effect on personal behavior.[37] For example, data aggregation now allows the connection bits and pieces of information like the purchase of cigarettes, what political party a person belongs to, the types of books purchased, etc. A portrait of a person could easily be drawn based on a few seemingly innocuous transactions of personal information.[38] The fear is that without proper regulation, these innocent transactions could have serious consequences for the individual. What would stop an unscrupulous insurance company from raising insurance premiums on individuals based on their food buying habits?

The supporters of information privacy assess the need for legal institutions to account for these new types of privacy intrusions by endorsing information self-determination. By giving people deference to the disclosure of personal information they are afforded greater control of their privacy. Proposals range from requiring consent to release information[39] to the commoditization of information which views information as personal property.[40]

---

[35] *See* Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW AND PHILOSOPHY 559, 584 (1998).
[36] Judith Wagner DeCew, *The Scope of Privacy in Law and Ethics*, 5 LAW AND PHILOSOPHY 145, 150 (1986).
[37] *See* Nissenbaum, *supra* note 35, at 593.
[38] *See Id.* at 589.
[39] *See, e.g.*, H.J. McCloskey, *Privacy and the Right to Privacy*, 55 PHILOSOPHY 17, 23 (1980).
[40] *See generally,* Francis S. Chlapowski, Note, *The Constitutional Protection of Informational Privacy*, 71 B.U. L. REV. 133 (1991).

Critics of information privacy will often cite that there are beneficial uses to collecting and analyzing information. Certainly in terms of national security there is an impetus to collect as much information as possible to root out potential criminals and terrorists. Likewise, one would not want privacy laws to hinder the disclosure of medical information during an emergency or the obstruction of financial information to evade paying taxes; on face value these types of information sharing are inherently positive. Richard Posner makes a convincing argument that in purely economic terms the concealment of information makes little sense.[41] He opposes information privacy because it creates inefficiency in the marketplace and refutes that protecting and concealing information in certain contexts could border on fraud (*e.g.*, it is not appropriate for a seller to conceal defects in a product, likewise a potential employee should not be able to conceal pertinent information from an employer).[42]

Other critics argue that information privacy is nothing new, but only builds upon and repackages existing arguments, as Ruth Gavison indicates, "part of the new interest in privacy is not caused by new needs, but rather by new doctrinal moves or hopes for legal change."[43] And indeed, many of the information privacy arguments do mirror or at least bare some resemblance to other arguments of privacy, but these critics underestimate the potential harm that could arise from information technologies. The exponential growth in computing power and the ever smarter artificial intelligences will likely create a new kind of intrusion that is far more disturbing than previously imagined. These new intrusions have necessitated an entirely new discourse and action in the privacy debate.

D. Privacy as a right or concept?

Lastly, there is some debate worthy of discussion regarding the notion or status of privacy. Privacy as a concept, interest, right, claim, principle, function, or value are just a few words present in the discourse. Since it is difficult to explain and define not all privacy scholars agree that it can be defined as a right. DeCew argues that calling privacy a right can be limiting and confusing and instead should be approached as an interest or

---

[41] *See* Richard A. Posner, *The Economics of Privacy*, 71 THE AM. ECON. REV. 405 (1981).
[42] *See id.* at 406.
[43] Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 466 (1980).

claim. She says that "I shall refer to privacy as an interest (which can be invaded), by which I mean something it would be a good thing to have, leaving open how extensively it ought to be protected."[44] Certainly categorizing privacy as a right has it problems since rights are often seen as absolute and the line between interests, legal rights, and moral or natural rights is not clear. DeCew attempts to remove the paradox of privacy as a right in order to simplify the argument of to what degree privacy should be protected, in this sense it makes no difference if privacy is a right or merely a claim. Kent Greenawalt further confuses the issue indicating that "privacy is not a claim; it is a situation or freedom about which claims may be made."[45]

There is some suggestion that privacy is not an independent right, but one derived from other rights. Warren and Brandeis looked to various issues from invasion of property rights to violations of contract to bolster that their "right to be left alone" ought to deserve its own standing.[46] Later, William Prosser would do the same by categorizing hundreds of cases into his four now famous privacy torts.[47] Judith Thomson suggests that are a cluster of rights that overlap with privacy because the line between the right in question and the right to privacy is vague. She affirms that "right to privacy" cases can be won without ever invoking privacy, but instead by invoking the true nature of the violation such as the right to bodily integrity or property rights.[48]

A legal right to privacy is often intangible because "the law's concern very reasonably has been with wrongful invasions of privacy, not with the philosophical question of what constitutes an invasion of privacy."[49] Nevertheless, the proponents of privacy as a right affirm that privacy is a basic need of man therefore should be treated as an intrinsic right. Glen Negley argues this point through his discussion of how societies value the individual. Although he affirms that morality of privacy and the individual are embroiled with historical relativity, he concludes that "if privacy is defined as an essential

---

[44] DeCew, *supra* note 36, at 147.
[45] Greenawalt, *supra* note 23, at 45.
[46] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 384 (1960).
[47] *See id.*
[48] *See* Judith Jarvis Thomson, *The Right to Privacy*, 4 PHILOSOPHY AND PUBLIC AFFAIRS 295, 312-13 (1975).
[49] McCloskey, *supra* note 39, at 18.

requirement for the achievement of morality, then privacy is a right that the law must protect and provide."[50] Lubor Velecky shares a similar opinion assuming that "laws ought to be made for the moral good of a community and the individuals in it. In this perspective a legal right to privacy exists only because the community in question has certain moral convictions about privacy as a moral good of its members."[51] Even though many theorists refuse to acknowledge privacy as a right, it should be noted that there is a large number of countries and international organizations that give privacy explicit constitutional protections and in some instances exalt it to the level of a fundamental human right.

The relationship between law and society is a crucial bridge to gap, for it is law that often reflects and in turn protects societal needs. Ruth Gavison argues that an explicit legal commitment to privacy is critical especially from social and technological changes, but also from the perspective that privacy stems from a moral institution.[52] In her analysis, she does not contend that privacy should be absolute, but it will have to be balanced with other values.[53] The advantages to an explicit commitment to "...privacy as a legal value may help raise awareness of its importance and thus deter reckless invasions."[54] It will serve to encourage the law to protect privacy in situations in which it is reluctant to do so, influence the law to presumptively favor privacy, and provide an educational element furthering the use and availability of privacy protections.[55] An explicit commitment and affirmation to legally protecting privacy will "remind us of the importance of privacy, and thus to color our understanding of protection in specific contexts."[56]

E. U.S. and European Concepts of Privacy

Despite all of the philosophical arguments for and against privacy, it is a particular society that ultimately decides how and why privacy is to be protected and valued. There

---

[50] Glen Negley, *Philosophical Views on the Value of Privacy*, 31 LAW AND CONTEMPORARY PROBLEMS 319, 325 (1966).
[51] Luber C. Velecky, *The Concept of Privacy*, in PRIVACY 23 (John B. Young ed., 1978).
[52] *See* Gavison, *supra* note 43, at 460.
[53] *See id.* at 467-8.
[54] *Id.* at 471.
[55] *See id.* at 470-1.
[56] *Id.* at 469-70.

is no better example of how two societies value privacy differently than that of the U.S. and Europe. Curiously though, the justifications and roots of privacy are not based on privacy at all, but two distinct cultural phenomena and historical antecedents. These cultural paradigms are distilled into the American view on liberty versus the European protection of dignity. Part of the reason that privacy is so prominently contested is due to the significance of liberty and dignity in the two respective cultures. In 1775 the call to arms of the American Revolution was "Give me Liberty or give me Death!"[57] Yet, Europeans equally revere their concept of dignity. Consider the following quotation from William Shakespeare:

> "Mine honor is my life; both grow in one;
> Take honor from me, and my life is done."[58]

It is clear that the concepts of liberty and dignity are not frivolously enshrined or respected.

The American revolutionary ideals and the later construction of the government framework emphasized righting the injustices suffered during the colonial period. The U.S. "is much more oriented towards values of liberty, and especially liberty against the state. At its conceptual core, the American right to privacy still takes much the form that it took in the eighteenth century: It is the right to freedom from intrusion by the state, especially in one's own home."[59] The gravity toward the ideals of liberty and distrust of government stems from this volatile period that still strongly resonate within American society. The realization that the protection of privacy by means of ensuring liberty (and vice versa) is key to understanding the way the U.S. views privacy. Consequently, most of the privacy protections in the U.S. concentrate on limiting government powers and minor prominence is placed on the private sector. Extensive personal information in the hands of private enterprise is of little concern to Americans compared to their unease with government information collection.[60] The importance of allowing the free flow of

---

[57] Attributed to Patrick Henry.
[58] WILLIAM SHAKESPEARE, KING RICHARD THE SECOND act I, sc. 1.
[59] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1161 (2004).
[60] Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 UTOLTJ 357, 387 (2005).

information is closely tied to the American view on freedom of speech and belief in the capitalist, market based economy.[61] Lastly, privacy rights in the U.S. are not considered absolute, privacy is constantly balanced with other competing rights.[62]

In Europe, dignity and honor are the driving forces behind the privacy debate. So much so that EU Charter of Fundamental Rights is founded on the basis of human dignity. Article one of the Charter states that "Human dignity is inviolable. It must be respected and protected."[63] The core principles of one's image, name, and reputation, and the desire to avoid humiliation are overriding concerns,[64] but further protections of personal information reflect the atrocities and experiences the Europeans experienced during World War II. Not wanting to repeat the abuses of data and authoritarian regimes similar to the Nazi occupation, strong privacy and human right protections prevail.[65] It would seem contradictory that the Europeans have given extensive powers to the government in protecting privacy in seeking to prevent authoritarian regimes, but this is more indicative of the legal structures and deference to the government being the guarantor of rights and the provider of essential services.[66] "[W]hen it comes to privacy, Americans generally do not assume that the government necessarily has citizens' best interests at heart...The European paradigm assumes a much higher comfort level with a far more authoritarian government."[67] Also, Europeans do not like the fact that businesses and corporations have access to personal information, therefore strong data protection directives regulate privacy as a fundamental and inviolate right, seldom trumped.

In conclusion, privacy whether a claim, concept, right, interest, or descriptive word will continue to be elusive, but its exact meaning is unimportant as long as privacy is

---

[61] Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 174, 220 (1999).
[62] DOROTHEE HEISENBERG, NEGOTIATING PRIVACY: THE EUROPEAN UNION, THE UNITED STATES, AND PERSONAL DATA PROTECTION 35-36 (2005).
[63] Charter of Fundamental Rights of the European Union, Dec. 18, 2000, 2000 O.J. (C 364/1), art. 1.
[64] *See* Avner, *supra* note 60, at 388.
[65] Michael W. Heydrich, Note, *A Brave New World: Complying With the European Union Directive on Personal Privacy Through the Power of Contract*, 25 BROOKLYN J. INT'L L. 407, 417 (1999).
[66] FRED H. CATE, PRIVACY IN THE INFORMATION AGE 44 (1997).
[67] Jane E. Kirley, *The EU Data Protection and the First Amendment: Why a "Press Exemption" Won't Work*, 80 IOWA L. REV. 639, 648-49 (1995).

universally accepted as a basic human need worthy of protection. Privacy is deeply connected to establishment of one's self, relationships, autonomy, and the control of personal information. Some argue that privacy is not limited to humans but a fundamental part of biological existence, bordering on an instinctual function of all animal life,[68] while others claim that privacy is a socially derived institution (logically, if society did not exist, then privacy would not be an issue).[69] The average person certainly does not need to understand the philosophical debate or care if privacy is a right or merely a concept, but he knows that privacy exists and that he is entitled to benefit from it.

Justice Potter Stewart once wrote the famous words of, "I know it when I see it,"[70] to determine the threshold of obscene content, but what he was actually attempting to express is an evident reality even though the categorization of the reality is subjective and lacks clearly defined parameters. This phrase could be used to describe the relativity of privacy. Conceptually and often legally privacy is difficult to define, but that does not prevent someone from knowing when his privacy has been infringed upon. Regardless of the country, society, culture, perception, or time period privacy has always existed and will continue to do so. As global interaction increases and unifies the different attitudes towards privacy, tensions and disagreements will arise that will have to be resolved and harmonized in order to foster efficient markets and to balance national security interests, while yet at the same time seeking to preserve the varying protections of individual privacy.

For the purposes of this essay it is not relevant to "choose sides" in the philosophical debate on privacy, but it would be helpful to decide on a determination of the word in order to reach a conclusion on the technological and security impacts in the current and future international legal organizations of the concept. Judith DeCew's definition of privacy as "whatever is not generally, that is, according to a reasonable person under normal circumstances, or according to certain social conventions, a legitimate concern of

---

[68] *See* Alan F. Westin, *The Origins of Modern Claims to Privacy*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 59 (Ferdinand D. Schoeman ed., 1984).
[69] CATE, supra note 66, at 22.
[70] Jacobellis v. Ohio, 378 U.S. 184, 197 (1964).

others because of the threat of scrutiny or judgment and the potential problems following from them"[71] seems practical, but lacks the importance that is placed on privacy as a prerequisite human need. In this sense it is crucial to view *privacy as necessary and grounded in basic morality* (regardless of society), almost *sui generis* in nature, but connected to the differing ideas of the concept of the person. The legal rights to privacy stem from this moral basis, but these legal rights are not absolute, therefore the question becomes not whether privacy as an institution or right exists, but to *what level should a democratic society should value and protect it?*

[71] DeCew, *supra* note 36, at 172.

III. The Legal Frameworks

In the international context, consensus on what constitutes the "legal right" to privacy has not been reached. Since privacy interrelates to historical, societal, moral, and political aims and differences, there has been no universally accepted definition or acknowledgement of how to view or regulate privacy. Ken Gormley notes that "legal privacy consists of four or five different species of legal rights which are quite different from each other and thus incapable of a single definition, yet heavily interrelated as a matter of history, such efforts to completely sever one from another are (and have been) disastrous."[72] Nevertheless, two competing legal regimes have emerged: the United States and European privacy models. While the U.S. and Europe are vying for dominance in the privacy debate, countries outside of these two legal regimes have had to choose sides and make difficult decisions on how to best protect their interests and maintain relationships with the two dominating privacy factions.

The U.S. and European privacy regimes have developed and evolved in separate directions and thus value and enact legal privacy protections differently, each seeking to balance the competing values that privacy influences. The U.S. model has been largely a sectoral, *ad hoc* approach, whereas the European model stresses the fundamental nature of privacy rights and enforces them from the top down in an *omnibus* fashion. These different legal approaches in combination with the philosophical leanings that the two regimes have towards privacy create distinctions that are beginning to collide as the world becomes more globally intertwined.

A. The US Perspective

The attitude in the United States towards privacy is an interesting dichotomy with no suggestion that privacy is granted the status of an absolute, inalienable right. In fact the word privacy is not mentioned at all in the U.S. Constitution, but instead privacy is derived and inferred from a number of constitutional amendments, Supreme Court decisions, tort protections, and an assortment of statutory laws. Even though privacy is not explicit it is often considered as important as any other fundamental rights and

[72] Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1339 (1992).

cherished vehemently. In 1776 the drafters of the Declaration of Independence eloquently established that "We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain *unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness*."[73] This concept and fervent protection of liberty are ideals present at all levels of American discourse and frequently elicited for the protection of privacy rights in the U.S. Arguably one of the most important inalienable rights for the pursuit of life, liberty, and happiness is the ability to mature independently and privately. It is with this frame of reference that has caused privacy to evolve and entrench itself into the heart of the most controversial issues that have shaped American life.

1. Constitutional framework

When deconstructing the right to privacy in the U.S. it is pertinent to first look at the constitutional protections. As previously mentioned, the word "privacy" does not appear in the Constitution, but privacy as a "right" is generally construed from the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments. Through the application of these amendments the Supreme Court attempts to bring certainty and predictability to how privacy rights are ordained. This is not an easy task since privacy issues have constantly surfaced in a wide variety of seemingly unrelated issues, but the relevant cases areas in understanding the evolution of U.S. privacy rights are found in three basic subject areas: the First Amendment cases, the Fourth Amendment cases, and the cases involving making intimate, fundamental decisions (invoking the Fourteenth and Ninth Amendments). Lastly, information privacy is in its infancy in constitutional jurisprudence, but ought to enjoy its own category in the future as its importance grows and with the resolution of additional cases.

a. The First Amendment establishes that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the

[73] THE DECLARATION OF INDEPENDENCE para. 2 (U.S. 1776) (emphasis added).

freedom of speech, or of the press; or the right of the people peaceably to assemble."[74] Inherent in the wide array of "free speech" principles ordained by this amendment are competing rights that must be balanced thus making privacy in this context murky and uneven. For example in *Stanley v. Georgia*,[75] the Court overturned the conviction of the possession of obscene materials, reasoning that free speech can be interpreted as the right to independent thought and dissemination. The justices affirmed that "if the First Amendment means anything, it means the State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional heritage rebels at the thought of giving government power to control men's minds."[76] The Court in justifying this right to free speech was required to invoke the protection of privacy rights. If the Court did not account for an individual's privacy, then free speech would be compromised.

In further cases, *Frisby v. Schultz*[77] upheld a Wisconsin ban on residential picketing citing that the State has an interest in protecting the privacy and tranquility of one's home. The Court often defers to the inviolability of one's home in free speech cases, but the absolute privacy of one's home is entirely situational. For example, in *Breard v. City of Alexandria*,[78] the Court overturned a local law forbidding door-to-door solicitation. In this case, the magazine salesman's right to free speech overrode the homeowner's right to privacy: "[T]he constitutionality of Alexandria's ordinance turn[s] upon a balancing of the conveniences between some householder's desire for privacy and the publisher's right to distribute publications in the precise way that those soliciting for him think brings the best results."[79] Other cases concerning the right to privacy in public have considered the content of the free speech and the offence to an individual's privacy. In these situations where free speech in public settings is at issue, privacy does not always prevail. So called "captive audience" cases highlight the balance between an individual's privacy and free

[74] U.S. CONST. amend. I. Religious and political freedoms are enumerated in this first amendment. Inherent in this right to free speech is the antithesis that one has the right not to speak
[75] *See* Stanley v. Georgia, 394 U.S. 557 (1969).
[76] *Id.* at 565.
[77] *See* Frisby v. Schultz, 487 U.S. 474 (1988).
[78] Breard v. City of Alexandria, 341 U.S. 622 (1951).
[79] *Breard*, 341 U.S. at 644.

speech. *Public Utilities Commission v. Pollak,*[80] for example, affirmed that music broadcasted on public street cars does not interfere with one's "right to be left alone," but if the music is "loud and raucous," then one might have grounds to invoke privacy protections.[81]

Closely related to the First Amendment cases are the tort remedies concerning privacy. Whereas constitutional privacy protects an individual from government intrusion, the torts inspired by Warren and Brandeis' law review article establish a remedy against intrusion from private individuals, especially the press. In some cases these torts must be balanced with the First Amendment's right of free press,[82] for example, should a newspaper have the right to publish the name of a rape victim that wishes to remain anonymous?[83] These torts were originally proposed and classified by William L. Prosser in 1960[84] and later incorporated into the Restatement (Second) of Torts.[85] The torts as a whole are considered one "invasion of privacy" tort, but are classified in four distinct torts:

1) Public Disclosure of Private Facts - The liability of publicly disclosing facts that are "highly offensive to a reasonable person" and that are "not of legitimate concern to the public."[86]
2) Intrusion upon Seclusion - "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[87]

---

[80] *See* Public Utilities Commission v. Pollak, 343 U.S. 451 (1952).
[81] Kovacs v. Cooper, 336 U.S. 77 (1949).
[82] The privacy interests in these cases involve the idea of anonymity balanced with the public's "right to know." *See* Eric Barendt, *Privacy and Freedom of Speech*, in NEW DIMENSIONS IN PRIVACY LAW: INTERNATIONAL AND COMPARATIVE PERSPECTIVES 11 (Andrew T. Kenyon & Megan Richardson eds., 2006).
[83] *See* The Florida Star v. B. J. F., 491 U.S. 524 (1989).
[84] *See generally* Prosser, *supra* note 46.
[85] RESTATEMENT (SECOND) OF TORTS (1977).
[86] *Id.* at § 625D. For more information on privacy torts, see Brian C. Murchison, *Revisiting the American Action for Public Disclosure of Private Facts*, in NEW DIMENSIONS IN PRIVACY LAW: INTERNATIONAL AND COMPARATIVE PERSPECTIVES 32 (Andrew T. Kenyon & Megan Richardson eds., 2006).
[87] *Id.* at § 652B.

3) False Light - This tort does not allow one to expose another in a false light. This false light would have to be "reckless" publicity that is "highly offensive to a reasonable person."[88]
4) Appropriation - "One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy."[89]

Since individual states are at liberty to define their own tort laws, there is no uniform application of the torts. Further, they are controversial in themselves since they are full of subjective interpretation and ambiguity. Nevertheless, they form a basis of what is deemed acceptable and appropriate behavior in regards to the conduct of private individuals and the dissemination of private information.[90]

b. The Third Amendment prevents the government from quartering soldiers in individual homes. It simply states that "No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law."[91] This amendment does not overtly allude to privacy, but it is another part of the argument to the constitutional sanctity the home.

c. The Fourth and Fifth Amendment Cases

The Fifth Amendment is a rarely contested right-to-privacy amendment. It establishes the privilege against self-incrimination: no person "shall be compelled in any criminal case to be a witness against himself."[92] Justice Bradley wrote that government acts of forced divulgement of information "may suit the purposes of despotic power; but it cannot abide the pure atmosphere of political liberty and personal freedom."[93] Thus, the right of a person to be secure in himself and not divulge incriminating evidence information is key not only to one's personhood, but to the very nature of a free society.

---

[88] *Id.* at § 652E.
[89] *Id.* at § 652C.
[90] For a general overview of many of these cases, see ELLEN ALDERMAN & CAROLINE KENNEDY, THE RIGHT TO PRIVACY (1995). Also see Murchison, *supra* note 86.
[91] U.S. CONST. amend. III.
[92] *Id.* amend. V.
[93] Boyd v. United States, 116 U.S. 616, 632 (1886).

Fourth Amendment, often in combination with Fifth Amendment, jurisprudence is perhaps the clearest and most evolved form of privacy protection constitutionally ordained; it is the quintessential expression of the revolutionary ideals crafted by the Founding Fathers to defend against the injustices suffered under colonial rule and is the seminal and most apparent source of privacy emanating from the Constitution. This right is expressed in the Bill of Rights as:

> the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[94]

The wording of this amendment strongly indicates the drafters' desire to provide broad protection, but at the same time limit the protection in a way that allows the State under certain circumstances means of intrusion. Some of the earliest Constitutional debates have centered around the meanings of the words found in this amendment and continue today as this right is sensitive to new technologies and law enforcement techniques.

Boyd v. United States,[95] decided in 1886, opened the Forth Amendment privacy debate and was influential in establishing the basis for the protection of government intrusion into the "sanctity of a man's home and the privacies of life."[96] The case involved the unlawful seizure of evidence and the governments attempt to compel the defendant to produce documentation later found to be protected by the Fifth Amendment. The Court found that the "...Fourth and Fifth Amendments run almost into each other" with the "...invasion of [the defendant's] indefensible right of personal security, personal liberty and private property..."[97]

But it was not until 1928 with the *Olmstead* decision that first major Forth Amendment controversy was debated. *Olmstead v. United States*[98] concerned the legality of wiretaps installed from the outside of a suspect's house (the law enforcement never trespassed

---

[94] U.S. CONST. amend. IV.
[95] Boyd v. U.S., 116 U.S. 616 (1886).
[96] *Id.* at 630.
[97] *Id.*
[98] *See* Olmstead v. United States, 277 U.S. 438 (1928).

onto the property in the installation of the wiretaps). The Court not wanting to expand the scope or meaning of the Fourth Amendment refused to acknowledge that telephone conversations in this case were protected. There was never any trespass, therefore there was never a violation of the Fourth Amendment. They reasoned that a person "who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside,"[99] and that Congress should legislate the admissibility of telephone communication rather than infer Fourth Amendment protection.[100] However, Justice Brandeis' dissent in this case would prove to be far more significant in future cases in his reaffirmation of his "right to be left alone." He argued that the Constitution must keep up with new innovations and that "every unjustified intrusion by the government upon the privacy of an individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[101] Brandeis understood the ramifications of technology and its impact on privacy: "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 of what is whispered in the closet."[102] He further asserted that:

> "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 feeling and of his intellect...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 left alone—the most comprehensive of rights and the right most valued by civilized man."[103]

His views would remain largely unheard until technology and privacy would collide again in *Katz v. United States*.[104]

The years leading up to the *Katz* decision would be crucial in influencing a pronounced shift in Fourth Amendment protections. In *Silverman v. United States*[105] the Court

---

[99] *Id.* at 466.
[100] Congress did react to the Olmstead decision in 1934 with the enactment of § 605 of the Federal Communications Act making wiretapping illegal. *See* 47 USCS § 605.
[101] *Olmstead*, 277 U.S. at 478 (Brandeis, W., dissenting).
[102] *Id.* at 473.
[103] *Id.* at 478.
[104] Katz v. United States, 389 U.S. 347 (1967).
[105] Silverman v. United States, 365 U.S. 505 (1961).

appeared to be loosening its rigid interpretation of the Fourth Amendment when it refused to allow evidence obtained with the use of a "spike mike," a microphone that utilized a house's heating duct to conduct sound waves from the private conversations inside. The justices affirmed that "at the very core [of the Fourth Amendment] stands the right of a man to retreat in his own home and there be free from unreasonable government intrusion."[106] This case, in conjunction with the widespread use of improving technologies, the strengthening of government powers under the leadership of J. Edgar Hoover, and security concerns of the Cold War, forced the Court to reevaluate the balance of Fourth Amendment protections.

The question confronting the Court in the *Katz* case specifically concerned the admissibility of evidence gathered from the wiretapping of a public phone booth, but generally they were forced with whether or not the Fourth Amendment can be broadened to include a far-reaching right of privacy. This case was unique in the fact that it once again broached to role of technology, but this time the invasion of privacy was in public, outside of the home. The Court reasoned that "the Fourth Amendment protects people, not places."[107] In this one sentence the justices would not only expand the scope of the Fourth Amendment to deal with the problem of new technology, but they would reject the "trespass doctrine" and expand protection to include areas that were outside of the previously accepted "zones" of privacy, *i.e.* one's home or papers. A new privacy test would be employed to control government actions: 1) "that a person have exhibited an actual (subjective) expectation of privacy" and 2) that the expectation be one that society is prepared to recognize as 'reasonable.'"[108]

Kyllo v. United States[109] is a recent Supreme Court case to wrangle with an emerging technology and its implications on the privacy rights of an individual. The case centers on the use of a thermal imaging device that was used in order to obtain a search warrant of a suspect's house.

---

[106] *Id.* at 511.
[107] *Katz*, 389 U.S. at 351.
[108] *Id.* at 361.
[109] Kyllo v. United States, 533 U.S. 27 (2001).

Danny Kyllo was engaged in a small marijuana growing operation based in his house. During the police investigation officers used the Agema Thermovision 210 thermal imager to confirm the existence of lamps used in the cultivation of the marijuana plants in the suspect's garage; the scan of the house, taken from across the street, showed unusually warm spots in relation to the rest of the house. This scan in conjunction with other evidence convinced a judge to issue a search warrant of the premises which confirmed the officers' original suspicions.

In the majority opinion Justice Scalia acknowledges that "it would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[110] He went on to further say that "the question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy."[111] The majority again looked at the *Katz* decision to determine what degree of privacy is reasonable in this circumstance. Plain view searches had long been upheld: basically if a police officer sees something out in the open, then he is allowed to investigate further without having to solicit for a warrant.[112] *Kyllo* brings up an entirely different issue as to whether searches could encompass a "sense-enhancing" technology that enabled the officers to "see" what was occurring inside the home.[113] The Government maintained that the thermal image search should be upheld since it only showed "only the heat radiating from the external surface of the house" [114] (thus in plain view). The majority, however, rejected this argument reasoning that the use of this

---

[110] *Id.* at 33.
[111] *Id.* at 34.
[112] *See* Harris v. United States, 390 U.S. 234 (1968) for the origins regarding the "plain view doctrine." Also, *see* California v. Ciraolo, 476 U.S. 207 (1986) for the Supreme Court's examination of plain view searches with the use of aerial surveillance. Even though the use of an airplane was novel in this case it is no different than seeing something in plain view from the street. "The Fourth Amendment protection of a home has never been extended to require law enforcement officers to shield their eyes when passing a home on public thoroughfares."
[113] Some sense-enhancing technologies have been found to be legal. The Court had previously broached this subject when the Environmental Protection Agency utilized commercial grade mapping cameras to document evidence. The Court upheld the cameras' use since the cameras merely enhanced human senses and did not reveal anything that could not have been normally seen. Also, the Court noted that the cameras were publicly available for use and purchase. *See* Dow Chemical Co. v. United States, 476 U.S. 227 (1986).
[114] *Kyllo*, 533 U.S. at 35.

technology is far too intrusive and could potentially reveal too many intimate details of a person's life within the confines of the sanctity of one's home and that this intrusion would not be obvious upon physical intrusion of the home. Also, relevant in its decision was the fact that thermal imaging is not in general public use. The Court seemed to struggle with how exactly to deal with the advancement of technology and the balance between government and private interests. On one hand, the Court wants to apply the *Katz* test to determine what would be a reasonable expectation of privacy, but in the end they seem to fall back on the pre-*Katz* doctrines of protected areas and the Trespass Doctrine.[115] Regardless of how they arrived at their decision, this case clearly expresses a sentiment that technology has a profound impact on privacy and the difficultly the Court has in determining the limitations that should be placed upon technology. This case will no doubt be one of many future cases examining the ramifications and effects that technology has already proven to have on privacy.

The preceding cases are just a few of the major decisions that the Court has made in support of privacy, but there have been a number of cases that question the commitment the Court has in regard to firm privacy protection. For example, in *California v. Greenwood*,[116] the Court found that there was no reasonable expectation of privacy in garbage left on the curb for collection. Also, in the wake of two other holdings, students and employees have reduced Fourth Amendment protections. *New Jersey v. T.L.O.*[117] held that probable cause is not required in student searches on school campuses and, at least for public sector employees, the Court found in *O'Connor v. Ortega*[118] that searches need to only be "reasonable." Lastly, in *Vernonia School District v. Acton*,[119] the Court has allowed blanket drug testing of student athletes. They determined that the school's policy was constitutional since there is a legitimate societal interest in preventing drug use, the fact that many athletes are role models on campus, and the unobtrusiveness of the searches countered a reasonable expectation of privacy. In light of these examples it is

---

[115] *See* David A. Sullivan, *A Bright Line in the Sky? Toward a New Fourth Amendment Search Standard for Advancing Surveillance Technology*, 44 ARIZ. L. REV. 967, 985 (2002).
[116] California v. Greenwood, 486 U.S. 35 (1988).
[117] New Jersey v. T.L.O., 469 U.S. 325 (1984).
[118] O'Connor v. Ortega, 480 U.S. 709 (1987).
[119] Vernonia School District v. Acton, 515 U.S. 646 (1995).

difficult to automatically assume that the Court will use the same standards of reasonableness in all situations. The Court's affirmation in the *Katz* decision that the Fourth Amendment "protects people, not places" does not seem to correlate to these situations.

d. Fundamental Decision Cases

Privacy in the context of making intimate, personal decisions is much different than the concept of privacy protected by the Fourth Amendment or tort law. The latter protections involve the actual intrusion by someone or some entity into an individual's life. The autonomy to make fundamental, intimate decisions is the essence of being human, it is the foundation of one's "personhood." Curiously, this concept is relatively young within U.S. constitutional law and is deeply connected to some of the most controversial issues present in societal debates. Thus, in the present context it raises profound questions of judicial activism, and has therefore been slow to develop while being approached with trepidation.

The explicit nature of privacy ordained in the Fourth Amendment against searches and seizures is much more tangible and discernable than the right to privacy found (and often overlooked as the prominent actor) in the Ninth and Fourteenth Amendments. The privacy derived from these amendments is implicit and only interpreted though "substantive due process." The Due Process Clause found in the Fourteenth Amendment[120] in combination with the people's reservation of rights in the Ninth Amendment[121] has allowed the Court to "find" or protect rights within the meaning of the term "liberty" that are not specifically mentioned in the Constitution or the Bill of Rights, but rooted in the interpretation of the Ninth and Fourteenth Amendments. Substantive due process has had it share of controversy throughout the years as opponents question the role of judicial activism and argue that it is beyond the scope of the Court's power to interpret rights that do not exist. This attitude is still quite prevalent in many of the

[120] U.S. CONST. amend XIV. Due Process Clause: Privacy in this clause is guaranteed from the concept of liberty and due process. "...nor shall any state deprive any person of life, liberty, or property, without due process of law..."

[121] U.S. CONST. amend IX. Rights retained by the people, "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."

fundamental-decision dissenting opinions where the more conservative members of the Court continue to argue that no where in the Constitution is there a general right to privacy.

For years the Court had been using substantive due process to justify a variety of decisions ranging from the right to teach foreign languages,[122] attend private schools,[123] and a host of labor decisions such as outlawing maximum-hours laws,[124] but it was not until 1967 that the Court finally used the Fourteenth Amendment to derive new privacy rights. In *Griswold v. Connecticut*[125] the Court was faced with striking down a Connecticut statue forbidding the use of contraceptives. In the landmark ruling the Court affirmed that a fundamental right to privacy exists. Justice Douglas reasoned in the majority opinion that the Bill of Rights has guaranteed various "zones of privacy" emanating from the "penumbras" of the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments.[126] Further, the Court seemed uneasy with the idea that the government should be able to intrude or regulate something as intimate as marriage: "Would we allow the police to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives? The very idea is repulsive to the notions of privacy surrounding the marriage relationship."[127]

In a concurring opinion three justices agreed that they should not only look at the Fourteenth Amendment's Due Process Clause as the legal facilitator of privacy in this case, but "they must look to the 'traditions and [collective] conscience of our people' to determine whether a principle is 'so rooted [there]...as to be ranked as fundamental.'"[128] Even thought the justices could not pinpoint exactly where the right to privacy is found in the Constitution they implied that privacy is more than a legal right, but a right "...older

---

[122] *See* Pierce v Society of Sisters, 268 U.S. 510 (1925).
[123] *See* Meyers v. Nebraska, 262 U.S. 390 (1923).
[124] *See* Lochner v. New York, 198 U.S. 45 (1905).
[125] Griswold v. Connecticut, 381 U.S. 479 (1965).
[126] *See Id.* at 484.
[127] *Id.* at 485-6.
[128] *Id.* at 493.

than the Bill of Rights."[129] This decision set the stage for one of the most controversial privacy cases the Supreme Court has argued – *Roe v. Wade.*

Roe v. Wade[130] is perhaps the most famous privacy rights cases in the history of the U.S., but most laypeople assume this case solely concerned abortion. *Roe v. Wade* was not solely about whether or not a woman has the right to terminate a pregnancy, but whether or not the government has the right to intrude into one's personal affairs and the ability to make intimate decisions. The court reasoned that "the right to privacy...is broad enough to encompass a woman's decision whether or not to terminate her pregnancy."[131] The Court made a huge leap from the traditional invocations of privacy in its past decisions when it allowed privacy to break free of the spatial constraints that had previously limited the application of privacy, some would argue that "the leap-frog from *Griswold* to *Roe* thus became the single most important burst in the history of twentieth century privacy."[132]

Even though the Court greatly enhanced the scope of privacy rights in the U.S. with the *Roe* decision, they also noted that this right is not absolute. "The Court's decisions recognizing a right of privacy also acknowledge that some state regulation in areas protected by that right is appropriate...the privacy right involved, therefore, cannot be said to be absolute."[133]

Lawrence v. Texas[134] marks the most recent Court intervention in privacy rights and builds upon past cases to bolster the position that there is a guaranteed right to privacy found within the Fourteenth Amendment. In this case the Court is asked to determine whether it is a "crime for two people of the same sex to engage in certain intimate sexual conduct."[135] Specifically the Court examined whether or not the Texas statute violated an individuals right to liberty and privacy protected by the Due Process Clause. Even though

---

[129] *Id.* at 486.
[130] *See* Roe v. Wade, 410 U.S. 113 (1973).
[131] *Id.* at 153.
[132] Gormley, *supra* note 72, at 1394.
[133] Roe v. Wade, 410 U.S. at 154.
[134] *See* Lawrence v. Texas, 539 U.S. 558 (2003).
[135] *Id.* at 562.

the Court is still divided on these controversial political and social issues that strike at the moral fabric of American society, they seem to be much at ease in invoking substantive due process claims in relation to privacy compared with the original case of *Griswold*, thirty-six years prior. Justice Kennedy speaking for the majority opens the opinion stating that:

> Liberty protects the person from unwarranted government intrusions into a dwelling or other private places. In our tradition the State is not omnipresent in the home. And there are other spheres of our lives and existence, outside the home, where the State should not be a dominant presence. Freedom extends beyond spatial bounds. Liberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct. The instant case involves liberty of the person both in its spatial and more transcendent dimensions.[136]

The zones of privacy and intimacy are much clearer in this opinion. Not only does the Court agree that there is a fundamental right to privacy, but they go on to further agree that these zone should be inviolate to state intrusion and extends the idea that liberty and autonomy (juxtaposed with privacy) are mutually inclusive and constitutionally protected. The majority could find "...no legitimate state interest which can justify its intrusion into the personal and private life of the individual,"[137] especially, as in this case, the private conduct involving two consenting adults.

Protecting the right to make fundamental decisions is a delicate struggle since the Court is constantly required to balance many controversial interests. Technologies, individual freedoms, morality, and social change are not fixed in time and seek to pressure traditions and create new mores and customs. The transition from the old to the new is not easy and the Court is still reluctant to broadly apply this right of privacy,[138] but it is clear that since the *Griswold* decision the Court has continued to strengthen the right to privacy derived from the concept of liberty found in the Fourteenth Amendment.

---

[136] *Id.* at 562.
[137] *Id.* at 578.
[138] In Washington v. Glucksberg, 521 U.S. 702 (1997), for example, the Court refused to overturn a ban on assisted suicide based on fundamental privacy claims.

e. Information Privacy Cases

Since the 1970s and the rapid acceleration of database technologies there has been much discussion of what protections individuals ought to have in regards to stored information. Even though the debate may be pervasive, there has been only one major U.S. Supreme Court decision in regards to the recent concept of information privacy.

Information privacy was first debated in *Whalen v. Roe.*[139] The plaintiffs sought to challenge the constitutionality of a New York statue enabling the collection and storage of "Schedule II" drug prescriptions in a government database. They argued that privacy should encompass: (1) "the individual interest in avoiding disclosure of personal matters" and (2) "the interest in independence in making certain kinds of important decisions."[140] The plaintiff's argued that the New York statute impaired both of the privacy interests.

In a unanimous decision the Court struck a blow to information privacy overriding privacy concerns in favor of a compelling State interest in preventing drug abuse. They did note that they are aware "of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files," that "the right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures," and that the "duty arguably has its roots in the Constitution,"[141] but where there are adequate protections of information, there is no invasion of privacy nor sufficient reason to curb the advancement of database technologies. It is important to stress the Court's acknowledgment of the overriding state interest in this case, *i.e.* drug abuse and regulation of controlled narcotics. It is unknown if the Court would have taken a different stand on the issue of information privacy if the state interest had been less pronounced.

Even though the subject has only been argued once, the Court did acknowledge that a constitutional interest in information privacy does exist, but this interest is limited to the

---

[139] *See* Whalen v. Roe, 429 U.S. 589 (1977).
[140] *Id.* at 599-600.
[141] *Id.* at 605.

purview of government dissemination of information and fell short of specifically recognizing a broad constitutional right.[142] Since *Whalen* the lower courts have been grappling with the individual's control over the disclosure of personal information and what responsibilities the government has to protect it, but no clear consensus has been reached.[143]

The lower circuits have adopted *Whalen* in varying degrees of scrutiny ranging from very strict interpretations to more balanced approaches. The some circuits require egregious violations of fundamental rights, where others are less stringent in determining what sorts of personal information are protectable.[144] The Third Circuit has adopted the "Westinghouse Test" in an attempt to employ a balanced approach in determining violations of information privacy which has also been utilized by other circuits.[145] The test weighs seven factors to justify whether an intrusion has occurred: (1) "the type of record requested"; (2) "the information it does or might contain"; (3) "the potential for harm in any subsequent nonconsensual disclosure"; (4) "the injury from disclosure to the relationship in which the record was generated"; (5) "the adequacy of safeguards to prevent unauthorized disclosure"; (6) "the degree of need for access"; and (7) "whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access."[146]

2. U.S. Statutory History

The statutory protections in the U.S. are numerous and cover many issues, but in the grand scheme do little to provide the average person with strong control over personal information or far-reaching protection. Many of the privacy regulations came about during the 1970s as the use of computers and databases became widespread and resulting

---

[142] Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 Berkeley Tech. L.J. 1085, 1125 (2002).
[143] *See* Daniel J. Solove, *MODERN STUDIES IN PRIVACY LAW: NOTICE, AUTONOMY AND ENFORCEMENT OF DATA PRIVACY LEGISLATION: Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1205-07 (2002).
[144] *See* Helen L. Gilbert, *Minors' Constitutional Right to Informational Privacy*, 74 U. CHI. L. REV. 1375, 1382 (2007).
[145] *Id.* at 1387.
[146] United States v. Westinghouse Electric Corp., 638 F.2d 570, 578 (1980).

from an influential report issued by the U.S. Department of Health Education and Welfare. This report recommended that a Code of Fair Information Practices be instituted to guide the government's collection and use of personal information. The basic principles urged in the report are:

> 1. there must be a way for an individual, to find out what information about him is in a record and how it is used;
> 2. there must be no personal-data record-keeping systems whose very existence is secret;
> 3. there must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent;
> 4. there must be a way for an individual to correct or amend a record of identifiable information about him; and
> 5. any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data. [147]

Since then there have been a number of important statutes that regulate how personal information is used, but it should be noted that virtually all of these statutory protections are geared towards regulating government activities and the protection of an individual's liberties vis-à-vis government intrusion, they do little to prevent private institutions from violating a person's privacy. Instead, the U.S. has adopted a *de facto* free market policy in regards to protecting privacy rights in the private sector relying on market based solutions, industry self-regulation, and consumer outcry to encourage companies to adopt and enforce good privacy policies.

The bulk of privacy regulations deals with government collection and use of information. Privacy Act of 1974[148] instilled the principles of the Fair Information Practices and sought to formally recognize the individual's interest in privacy and the legitimate government interest in collecting personal information. U.S. Congress found that "the increasing use of computers and sophisticated information technology...has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information."[149] As a result Congress

---

[147] *See* U.S. Department of Health, Education and Welfare, *Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and Rights of Citizens,* iii (1973).
[148] 5 U.S.C. § 552a.
[149] Pub. L. No. 93-579, 90 Stat. 1198, at § 2(a)(2).

acted to regulate the information contained by federal agencies in order to preserve individual privacy. The basic provisions of the act allow an individual to access personal records[150] and provide mechanisms for the correction of erroneous data.[151] The federal agencies in turn must only collect and use information for its stated purposes,[152] reasonably maintain the accuracy and relevancy of collected information,[153] and establish appropriate safeguards to preserve the confidentiality of the information.[154]

Other statutory protections have been created on a sector-by-sector approach to protect specific privacy interests in the nongovernmental realm. These regulations are often enacted to react to new technologies and other threats to privacy. A famous example of this *ad hoc* approach was the passage of the Video Privacy Protection Act of 1988.[155] During Judge Robert Bork's Senate confirmation hearings an enterprising member of the press was able to obtain and release the Supreme Court nominee's video rental records. An outraged Congress quickly reacted to this privacy intrusion by regulating the disclosure of such information. It is indicative of the U.S. approach to privacy control by passing a very specific piece of legislation, covering narrow actions. Other examples of private industry regulations include: the Fair Credit Reporting Act of 1970[156] which regulates the responsibilities of credit reporting agencies in the maintenance and accuracy of credit reports; the Children's Online Privacy Act of 1998[157] prohibits the collection of online information about children under the age of thirteen; the Cable Communications Policy Act of 1984[158] regulates records maintained by cable companies; the Employee Polygraph Protection Act of 1988[159] prohibits the use of polygraphs by private employers; and the Health Insurance Portability and Accountability Act of 1998[160] governing the privacy of medical records. This list is a fraction of the statutes protecting

---

[150] *See id.* at § 2(b)(1).
[151] *See id.* at § 2(b)(3).
[152] 5 U.S.C. § 552a (e)(1).
[153] 5 U.S.C. § 552a (e)(5).
[154] 5 U.S.C. § 552a (e)(10).
[155] 18 U.S.C. §§ 2710-2711.
[156] 15 U.S.C. §§ 1681-1681t.
[157] 15 U.S.C. §§ 6501-06.
[158] 47 U.S.C. § 551.
[159] 29 U.S.C. §§ 2001-2009.
[160] Pub. L. No. 104-191, 110 Stat. 1936.

privacy and is meant to only show the general, patchwork nature of privacy regulation on at the U.S. federal level.

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("Patriot Act")[161] was passed shortly after 9/11 in response to the terrorist attacks. Critics of the Patriot Act highlight its notable impacts on civil liberties, especially privacy since the act greatly expands police surveillance capabilities and investigative authority.[162] The passage of the anti-terrorism bill was done with great pressure, virtually no debate or deliberation, and with no assurance that the loss of civil rights would equate to greater security.[163] Many would see the Patriot Act's passage as a too hasty, knee-jerk response to a national security crisis rather than sound legislative discussion since many of its provisions had been previously rejected by Congress.[164]

The Patriot act primarily updates and incorporates new surveillance techniques into existing law. Section 206, for example, broadens the scope of foreign surveillance to include domestic surveillance by amending portions of the Foreign Intelligence Surveillance Act.[165] Section 216, amending the Electronic Communications Privacy Act, allows "pen registers" to be expanded from merely telephone communication to include all computer based communications.[166] But most notable is that the Patriot Act lowers the minimum standards for the production and collection of evidence, in some cases completely eliminating the need to show probably cause.[167] Even though the Bush Administration asserts that the Patriot Act is absolutely essential for fighting terrorism, many believe that the government has begun to use the law in many cases that have no

---

[161] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) [hereinafter "Patriot Act"].
[162] *See* John R. Soma et al., *Balancing of Privacy vs. Security: A historical Perspective of the USA PATRIOT Act*, 31 RUTGERS COMPUTER & TECH. L.J. 285, 307 (2005).
[163] *See* Sharon H. Rackow, *How the USA Patriot Act Will Permit Governmental Infringement Upon the Privacy of Americans in the Name of "Intelligence" Investigations*, 150 U. PA. L. REV. 1651, 1652 (2002).
[164] *See* Soma, *supra* note 162, at 308.
[165] *See id.* at 310.
[166] *See id.* at 311-2.
[167] *See id.* at 313.

connection to terrorism.[168] This is particularly startling when viewed with the expanded domestic surveillance powers previously reserved for monitoring foreign nationals outside of the U.S. and have caused many to question the constitutionality of some of the Patriot Act provisions.

To conclude, technological and historical triggers as well as societal transformations often precede new questions regarding privacy rights. For this reason, and the fact that privacy is so hard to define within the American legal system, future manifestations of privacy rights will be largely unexpected and unpredictable. As new gaps in privacy rights are found the judicial process will attempt to repair the holes by finding new rationales and interpretations within the loosely construed meanings of the Constitution and the legislature will continue to create new protections in the form of statutory regulation.

Whether or not one believes that there is a distinct right to privacy protected in the U.S. is still up for debate as some would still argue that this right is invented by activist judges. They would argue that privacy is not a stand alone right and should be accurately described as a general right to liberty, but nevertheless many of the privacy cases do show a distinct, inclusive privacy right that has evolved and is symbiotic with the ideals of liberty present in American discourse.[169] Judging from some of the decisions and rhetoric it appears that privacy is slowly moving away from a nonexistent right to a fundamentally protected right within U.S. Constitutional jurisprudence. Moreover, the body of U.S. statutory regulations is beginning to encompass more private sector control and privacy protections as the law adapts to the Information Age and increased global interaction, but conversely, issues of national security seek to pressure government transgression into personal privacy and civil rights with the passage of legislation such as the Patriot Act.

---

[168] *See id.* at 337.
[169] *See generally* Whitman, *supra* note 59.

B. European Union Framework

The European privacy model contrasts sharply with that of the U.S. as they view the right to privacy in a much more fundamental way and have strived to incorporate this ideal in a comprehensive fashion throughout European legislation. Europe's commitment to privacy (especially information privacy) is not new, the first privacy regulations occurred in Europe and the protections in place today are not surpassed by any other privacy regime.[170] This fundamental privacy right is often referred to a "data protection" in European dialogue rather than merely "privacy." This stems from a broader adoption of modern ideals of informational privacy and the concept that individuals ought to have a large degree of control and protection of the dissemination of their personal information. Whereas the U.S. uses a market-based approach for protecting privacy, Europe views the State as an important actor in upholding privacy as a critical element in the social construct of European life. Unlike the U.S. model which mainly focuses on the government's information gathering and intrusion, the European data protection directives make no distinction between the private and public dissemination of information. Businesses and governments alike have to follow the same rules. The data directives apply not only to information collected and located within the confines of Europe, but also has an extraterritorial effect regulating any data that is exported to other countries.[171] Further, individual control of information is much greater as European privacy rights embrace the concept of "information self-determination."[172] By recognizing privacy as a fundamental right, a burden is placed on the entities who want the information to prove that there is a substantial need for such information rather than the individual having to fight for the right not to disclose the information.[173]

1. Privacy as a Fundamental Human Right

The fundamental nature of privacy rights as a human right stems from the United Nations Universal Declaration of Human Rights created in 1948. This affirmation of human rights

---

[170] CATE, *supra* note 66, at 47.
[171] Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 174, 179 (1999).
[172] Joe R. Reidenburg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 730-31 (2001).
[173] Nissenbaum, *supra* note 35, at 594.

was largely a result of atrocities committed during World War II and seeks to acknowledge the "recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world."[174] Article 12 of the U.N. Declaration states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."[175]

The European Convention on Human Rights (ECHR) created in 1950 furthers the ideals outlined in the U.N. Declaration. Its stated goal is to "secure the universal and effective recognition and observance"[176] of the rights elaborated in the convention, but it also resolves to ensure the collective enforcement of these rights through the establishment of the European Court of Human Rights.[177] Article 8 of the ECHR specifically deals with privacy by asserting that:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[178]

Since the ECHR adoption the member states have diligently attempted to fulfill this privacy objective. These efforts resulted in the adoption of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1980 Convention) in 1980,[179] but since the convention was not self-executing and definitions to important elements not clear, its enactment was either nonexistent or inconsistent among the EU member states.[180] For these reasons the European Union Data Protection

---

[174] Universal Declaration of Human Rights, pmbl., G.A. res. 217A (III), U.N. Doc. A/810 (Dec. 12, 1948).
[175] *Id.* art. 12.
[176] Convention for the Protection of Human Rights and Fundamental Freedoms, pmbl., Nov. 4, 1950, Europ. T.S. No. 5 [hereinafter CPHR].
[177] *See* CPHR art. 19.
[178] CPHR art. 8.
[179] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, Europ. T.S. No. 108. [hereinafter 1980 Convention]
[180] *See* CATE, *supra* note 66, at 34.

Directive of 1995 (Directive)[181] was culminated, forcing the states to enact a comprehensive set of rules to harmonize the regulatory framework of information flows and the protection of personal privacy.

2. The Data Protection Directives

Clearly, Europe has become the champion of privacy rights in the digital age. The acknowledgment of privacy as a human right coupled with the modern legislation concerning data flows allows the individual unprecedented protection. Data protection was first introduced with the adoption of the 1980 Convention and set out a number of basic principles requiring that automatically processed data be:

1. obtained and processed fairly and lawfully;[182]
2. Stored for specified and legitimate purposes;[183]
3. adequate, relevant and not excessive in relation to the purpose for which they are stored;[184]
4. accurate and, where necessary, kept up to date;[185]
5. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored;[186]
6. protected by appropriate security measures from accidental or unauthorized loss, destruction, access, alteration, or dissemination;[187] and
7. that individuals be allowed to access and amend incorrect data.[188]

These principles would be incorporated in later European privacy regulations as well as the Organization of Economic Co-operation and Development's Guidelines on the Protection of Personal Privacy and Transborder Flows of Personal Information (OECD Guidelines).[189] The guidelines established nonbinding recommendations and principles regarding data protection and the free flow of information across international borders.

---

[181] Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing Personal Data and on the Free Movement of Such Data, October 24, 1995, 1995 O.J. (L281/31). [hereinafter Directive 95/46/EC]
[182] 1980 Convention, art. 5(a).
[183] 1980 Convention, art. 5(b).
[184] 1980 Convention, art. 5(c).
[185] 1980 Convention, art. 5(d).
[186] 1980 Convention, art. 5(e).
[187] 1980 Convention, art. 7.
[188] 1980 Convention, art. 8.
[189] OECD, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (2002).

The importance of the principles laid out in the 1980 Convention and the OECD Guidelines would not be felt until the adoption of the Directive 95/46/EC.[190]

The Directive 95/46/EC was formally approved on October 25, 1995 and with its enactment three years later set a high standard for privacy protection with its overall breadth and comprehensiveness. It represents the latest attempt to safeguard individual privacy and freedom in light of constantly advancing technologies.[191] Further, the Directive is a manifestation of the commitment the member states have towards privacy as a basic human right, on the same level as other basic rights such as freedom of expression. The objective of the directive is two-fold: (1) "Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data" [192] and (2) "Member States shall neither restrict nor prohibit the free flow of personal data between Member States..."[193] Thus not only would privacy be increased within Europe, but the directive would help fulfill the goal towards creating a single, integrated market.

The Directive elaborates minimum standards which the member states must use in their enabling legislation on the processing of personal data. It defines the processing of personal data very broadly to include "any operation or set of operations which is performed upon personal data, whether or not by automatic means."[194] Likewise, "personal data" is equally general in meaning: "any information relating to an individual or identifiable natural person ... in particular to reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[195] The Directive makes no distinctions to whom the law applies. Businesses and governments alike must follow the same rules, although activities performed in the course of security and criminal law and by "natural person[s] in the

---

[190] *See* Ulrich U. Wuermeling, *Harmonization of European Union Privacy Law*, 14 J. MARSHALL J. COMPUTER & INFO. L. 411, 416 (1996).
[191] *Id.* at 413.
[192] Directive 95/46/EC, art. 1 § 1.
[193] Directive 95/46/EC, art. 1 § 2.
[194] Directive 95/46/EC, art. 2(b).
[195] Directive 95/46/EC, art. 2(a).

course of purely personal or household activit[ies]" are outside the scope of the directive.[196]

The basic protections enumerated in the directive provide that the member states must insure that data is accurate, up-to-date, and collected for its intended use. Further, the data must be relevant and not excessive and only kept for the duration of the specified use.[197] On a personal level the Directive allows the individual not only to give consent to the use and gathering of information,[198] but also the right to access the information to correct errors.[199] Lastly, the collected data must be protected from "accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, ...and against all other unlawful forms of processing."[200]

Whereas one of the main goals of the Directive is to harmonize privacy laws in Europe, the implementation of the Directive has not been perfect. The requirement that each country change its national laws to comply with the Directive has not been smooth, partly because each country is able to interpret and enact the provisions differently based on each individual country's legal system.[201] The loopholes created with the overly general exemption clauses (such as national security, criminal investigations, and public health) could create further tension in the unification of privacy laws within Europe.[202]

3. Article 25: International Flows of Information

Directive 95/46/EC accomplished more than the domestic regulation of privacy within Europe, it created a standard of information sharing exported to jurisdictions outside the confines of the European Union. Article 25 of the directive specifically deals with transnational information flows:

---

[196] Directive 95/46/EC, art. 3 § 2.
[197] Directive 95/46/EC, art. 6 § 1(a)-(e).
[198] Directive 95/46/EC, art. 7(a).
[199] Directive 95/46/EC, art. 12.
[200] Directive 95/46/EC, art. 17 § 1.
[201] *See* Wuermeling, *supra* note 190, at 459.
[202] *See id.* at 460.

> the Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.[203]

With the enactment of this article in 1998 a potentially enormous transatlantic conflict with the United States was created that put the two very different privacy regimes at odds with each other. The importance of the 1998 conflict was the scope of the economic ramifications of not finding a common ground – it was estimated that $120 billion dollars in trade was put in jeopardy.[204] Also, a similar conflict in 2003 concerning the collection of Passenger Name Record data for airline passengers risked the shut down of air traffic between the two continents.

But the conflicts were not just about economics, they were the reflection of two competing viable perceptions of privacy. The European Union model focuses on a comprehensive, omnibus framework imposing strict rules that made no distinctions between private or public dissemination of data. Privacy in the European context is a fundamental human right, therefore nonnegotiable. In contrast, the U.S. has instituted a sectoral approach to regulating privacy with a focus on restricting the collection and intrusion of the government. Private-sector processing of personal data is allowed great freedom to let the market and self-regulation dictate its behavior. On one hand, the Europeans only wanted to uphold their standard of privacy protection, but this standard was incompatible with the U.S. system. Singling out only European data in the U.S. to ensure compliance to the directive was impractical, if not impossible. Moreover, it was not realistic that the U.S. completely change its entire system to comply with the Directive 95/46/EC.[205]

A catch-22 situation transpired into a diplomatic conflict with both sides having equivalent power, unwilling to compromise their respective positions, and each seeking to be the dominant actor. Regardless of the profound differences in core privacy principles, both sides had a considerable interest in seeking resolution. U.S. companies

---

[203] Directive 95/46/EC, art. 25 §1.
[204] *See* HEISENBERG, *supra* note 62, at 2.
[205] *See* HEISENBERG, *supra* note 62, at 2-3.

worried about the disclosure requirements and economic costs of the Directive's implementation,[206] while the Europeans were anxious that the business relationships and access to the U.S. market would be severely restricted,[207] in addition to protecting the fundamental privacy of their citizens.

Resolving the conflict would be limited. Typically, in trade related matters, the logical dispute resolution forum is through the auspices of the World Trade Organization, but in the general trade exceptions of the WTO General Agreement on Trade in Services (GATS) "the protection of privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts" is specifically exempted to member states.[208] Discussions would finally occur in 1999 and a year later a compromise negotiated with the adoption of the "Safe Harbor Principles." The principles are designed to allow U.S. companies to provide "an adequate level of protection" to European data through a self-certification that they are taking the necessary protection measures and agree to certain enforcement measures to ensure proper compliance.[209] Although the compromise allowed commerce to continue, it is largely seen as a "cease fire" with neither side really winning the privacy debate.[210] The U.S. was allowed to continue its self-regulatory approach to privacy, whereas the EU's privacy concerns were somewhat appeased.

This case highlights the growing concerns that the regulation of privacy is increasingly becoming a "disruptive force in the planning and operation of sound information technology practices" as businesses are forced to act in accordance with to the various domestic and international rules on privacy.[211] The ramifications of having multiple privacy regimes forces companies and countries to adjust their practices if they intend to

---

[206] *See* Morey Elizabeth Barnes, *Falling Short of the Mark: The United States Response to the European Union's Data Privacy Directive*, 27 NW. J. INT'L L. & BUS. 171, 179 (2006).
[207] *See* Cate, *supra* note 61, at 229.
[208] General Agreement on Trade in Services, art. XIV (c)(ii).
[209] U.S. DEP'T OF COMMERCE, SAFE HARBOR PRINCIPLES, July 21, 2000, http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm.
[210] *See* HEISENBERG, *supra* note 62, at 4.
[211] Jeffrey B. Ritter, Benjamin s. Hayes, & Henry L. Judy, *Emerging Trends in International Privacy Law*, 15 EMMORY INT'L L. REV. 87, 104 (2001).

do business with one of the major privacy regimes. Some commentators have noted that "achieving alignment with the European Union on the privacy issue has been considered an important bridge toward increased economic opportunities with the lucrative European market."[212] While others acknowledge the explosion of countries passing privacy laws mirroring the principles of the European data protections indicates that the EU privacy regime has become "the de facto international standard."[213]

The EU had the advantage of being the "first mover" in establishing comprehensive, internationally compulsory privacy legislation forcing outside countries to adopt comparable privacy protections in order to continue business relations within Europe.[214] The United States was at a disadvantage in its negotiations with the EU in regards to transborder flows of information. Not having a viable, competing privacy model the U.S. was forced to on some levels yield to the demands of the Directive with the adoption of the Safe Harbor Agreement.[215] Yet, the later conflict over airline passenger information has created doubt in the solidarity of Europe's power over privacy. Most European airlines had already capitulated to U.S. demands in disregard to the data directives which aiding the U.S. in unilaterally forcing the EU into submission.[216] Even though the U.S. has been reluctant to bend to European pressure, the EU has used it market power and "critical mass" to force many other countries opt for and implement adequate privacy controls mirroring the European model rather than the self-regulatory system that the U.S. has defended.[217]

---

[212] *Id.* at 104.
[213] *See* HEISENBERG, *supra* note 62, at 169.
[214] *See* Heisenberg, *supra* note 62, at 169-70.
[215] *See id.* at 67.
[216] *See id.* at 154.
[217] *See id.* at 120.

IV. New Threats to Privacy

Most of the international disputes over privacy involve the sharing, distribution, and dissemination of personal data, but there are other concerns that transcend national borders as governments are increasingly utilizing new tools to spy on their citizens and those of other countries in the name of national security and anti-terrorism. As new technologies are developing there is an international trend to use these technologies locally, such as the use of surveillance cameras, and globally, such as data mining and eavesdropping operations being conducted on an international and domestic level. Other technologies such as biometrics and RFID chips have the potential to seriously impinge the autonomous function of privacy. Justice Brandeis understood the implications of technology in 1928 when he said that "the progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping...Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts, and emotions...Can it be that the Constitution affords no protection against such invasions of individual security?"[218]

Today, his warning resonates with the advances in technology, but his question as to the protection afforded by the Constitution seems to fall on deaf ears. Even though a particular government or privacy regime may say they are concerned with the individual's privacy rights, they are doing very little to slow the development of dangerous technologies or at the very least allow for information and dialogue to be shared so that a meaningful public debate can take place. In the post 9-11 world governments are using the risk of terrorism to quickly and often secretly employ new technologies and methods to invade individual's privacy with little or no public scrutiny. The "shoot-first-ask-questions-later" policies that law enforcement and intelligence agencies are employing in regards to privacy issues could be detrimental to current and future protections.

[218] *Olmstead*, 277 U.S. at 474 (Brandeis, S., dissenting).

A. Mass Surveillance

Shortly after the terrorist attacks on the World Trade Center on September 11, 2001 the attitude towards privacy drastically changed. The U.S. came to the realization that the terrorists who carried out the attacks lived and operated within U.S. borders. Law enforcement authorities and the intelligence community have used the aftermath of 9/11 and the resulting political drive to strengthen national security and enact new powers, greatly expanding the government's surveillance capabilities. The Patriot Act was the progeny of the post-9/11 political debate and has sparked considerable criticism that it gives the government too much power and weakens civil liberties.

With the passage of the Patriot Act, legislation now allows intelligence interests far-reaching and unprecedented access to private records and communications. Some argue that the movement to increase the scope of surveillance capabilities and engage in new espionage technologies was already in place before the attacks -- the intelligence community was merely waiting for the opportune moment to expand their powers.[219] The Bush administration has continuingly justified the 9/11 attacks as validation for its expanded powers, but allegations have recently surfaced that the National Security Agency (NSA) approached Quest Communications six months before the 9/11 attacks with a potentially illegal wiretapping scheme.[220] Most likely, the push for increased intelligence powers would have happened regardless of the 9/11 attacks, but instead, the attacks have created an atmosphere of fear and panic and an urgency to give unbridled power to intelligence agencies without proper public discourse and common sense. The secrecy of the new powers and the use of National Security Letters, for example, prevent the public from knowing what sorts of activities the government is engaging in and the lack of discourse and oversight has created severe doubt as to whether or not privacy interests are being appropriately handled.

A recent high profile data breach at the U.S. State Department involved the unauthorized viewing of the passport files of the three leading presidential candidates and other

---

[219] JAMES B. RULE, PRIVACY IN PERIL 55 (2007).

[220] *See* Ellen Nakashima & Dan Eggen, *Former CEO Says U.S. Punished Phone Firm: Quest feared NSA Plan Was Illegal, Filing Says*, WASH. POST, Oct. 13, 2007, at A1.

celebrities.[221] Further, a 2007 data breach in Britain is being hailed as the worst privacy breach ever. The British tax authorities copied data, including bank account numbers and information on almost every British child under the age of sixteen, onto unencrypted disks which were subsequently "lost in the mail."[222] These examples show not just the disregard and vulnerability for data security, but also the ineptness of the people entrusted to keep sensitive information safe. Securing data is only a partial answer to information privacy, limiting the amount and types of data collected and stored is actually the superseding issue.

The collection and analysis of information is not the only part of the mass surveillance networks being created. Basic surveillance technologies like cameras are becoming more hi-tech and specialized. The transition from simple Close Circuit Television to large-scale networked digitalized systems utilizing biometric technologies and other behavioral identification techniques raises new privacy concerns.

1. Cameras

Cameras are everywhere. Mass observation is now the norm in modern societies as law enforcement and private actors have employed sophisticated camera networks in the aims of public safety and protection of private property. Major cities across the globe have installed Close Circuit Television Systems (CCTV) that constantly monitor and record their surrounding twenty-four hours a day. It is estimated that there are 4.2 million CCTV cameras in the U.K. (one for every 14 people), filming the average Britain over three hundred times per day, at a cost of almost one billion dollars since the 1990's,[223] this includes central London's "Ring of Steel" which employs over 500,000 cameras alone. Camera use in the United States is not yet as pervasive as in the U.K., but there are huge initiatives across the country to build extensive, high-tech video surveillance systems to combat terrorism and other crimes. Washington D.C. announced that it will consolidate over 5,000 cameras operated by multiple agencies under the city's Homeland Security

---

[221] *See* Helene Cooper, *Passport Files of 3 Candidates Were Pried Into*, N.Y. TIMES, Mar. 22, 2008, at A1.
[222] *See* Eric Pfanner, *Britain Apologizes for Major Data Breach; 25 Million People May Have Been Affected*, INT'L HERALD TRIB., Nov. 23, 2007, § News, at 5.
[223] SURVEILLANCE STUDIES NETWORK, A REPORT ON THE SURVEILLANCE SOCIETY 19 (2006).

Agency.[224] The Metropolitan Transportation Authority of New York City is attempting to secure its transit network with a next-generation surveillance system that will use video algorithms to spot suspicious behavior.[225] Some camera systems are going one step farther by installing two-way communications that not only allow the operator to listen to street conversations, but will also allow the cameras to talk back and reprimand bad behavior.[226] By 2013, the market for video surveillance technologies is expected to grow from $13.5 billion in 2006 to $46 billion dollars per year.[227] Moreover, the use of CCTV systems is completely legal since it is bolstered by the argument that people should not have any expectations of privacy in public settings. While to a certain extent this argument may be valid, the pervasiveness of video surveillance and loss of anonymity while in public cause many to question the use of mass surveillance.

A recent study shows that San Francisco's anti-crime cameras have had no effect on reducing violent crime. The report suggests that murders, for example, decreased within the camera's range, but was offset by an increase in murders further away – people just moved down the street before killing each other.[228] Figures in London are not much better. In areas blanketed with security cameras crime resolution rates are below average with eighty percent of crimes remaining unsolved.[229] Public safety officials continually point out that the cameras are primarily for public health and safety and that police cannot be everywhere at once, but critics of the cameras say that the statistics used by the proponents are misleading since they do not account for the displacement of crime outside of the cameras range and other questions as to the effectiveness and cost-to-benefit ratio of mass surveillance are still unresolved.

---

[224] *See* Gary Emerling, *5,000 Monitoring Cameras Opened to D.C. Police; Rights Group Hit Expansion*, WASH. TIMES, Apr. 9, 2008, at A1.
[225] *See* Kathleen Lucadamo & Pete Donohue, Get *the Cameras Before Terrorists Hit Again*, DAILY NEWS (N.Y.), Oct. 3, 2007, § News, at 10.
[226] *See* Peter Morrell, *Watched and Now Listened To, Is Privacy a Thing of the Past?*, THE WESTERN MAIL (WALES), May 24, 2007, § News, at 22.
[227] Press Release, ABI Research, Video Surveillance: A Market Poised for $46 Billion of Explosive Growth (Mar. 18, 2008) (http://www.abiresearch.com/abiprdisplay.jsp?pressid=1081).
[228] *See* Heather Knight, *Crime Cameras Not Capturing Many Crimes*, S. F. CHRON., Mar. 21, 2008, at A1.
[229] Justin Davenport, *Tens of Thousands of CCTV Cameras, Yet 80% of Crimes Unsolved*, EVENING STANDARD (LONDON), Sept. 19, 2007.

The digital camera market has skyrocketed in the recent years. More than half of U.S. households own digital cameras taking over thirty-four billion pictures per year.[230] Flickr, a popular internet picture hosting site, indicates that over two billion user photos have been uploaded to its site.[231] The use of digital cameras powered by the internet has made photographs easily accessible worldwide. Society, especially the younger generations, is quickly adapting to the new technology digitally recording all aspects of life. Consumers may think that uploading photographs poses little risk to their privacy, but new facial recognition software is now able to search online databases and "tag" names to the people featured in supposedly anonymous photos.[232] Privacy concerns involve the involuntary disclosure of one's image and whether or not a person has the right to control the dissemination of his image or likeness. Privacy torts have protected people from these sorts of transgressions in the media, but questions remain if the same torts can protect the privacy of individuals in the openness of the internet age. The loss of autonomy and potential for every humiliation to be documented on video could have huge impacts on the way people interact with each other.

Cameras are being embedded in a wide variety of consumer goods. Hidden cameras and so called nanny-cams are secretly and illegally videotaping people without their knowledge. Digital cameras are integrated into many cellular phones, causing them to be banned in many places where people expect a high degree of privacy like gyms and locker rooms. And cameras and microphones embedded into laptop computers could soon spy on you. Google has announced plans to develop "ambient audio listening technology" to activate computer microphones to personalize advertising. For example, if Google hears an identifiable sound like a dog barking, then a dog food advertisement would appear.[233] It would not be a stretch of the imagination to believe that governments already have the capability to do the same. The use of Trojan horses or other backdoors into one's computer by the government or any other savvy computer hacker can turn a

---

[230] Janet Kornblum, *Always in the Camera's Eye*, USA TODAY, May 27, 2006, at D1.
[231] Press Release, Yahoo! Inc., Flickr Adds Video to its Popular Photo-Sharing Community (Apr. 8, 2008) (http://yhoo.client.shareholder.com/press/releasedetail.cfm?ReleaseID=303857).
[232] 2006 Oliver Wendell Holmes Lecture, *In the Face of Danger: Facial Recognition and the Limits of Law*, 120 HARV. L. REV. 1870, 1871 (2007).
[233] Abbey Klaassen, *Listen to This: Google Plan Lets Laptops Hear Your TV*, ADVERTISING AGE, June 26, 2006, at 3.

computer into a virtual surveillance device. Germany has recently been criticized for sending Trojan horse viruses to suspect computers that allow the government unfettered access without the owners' knowledge, the privacy risks are already a reality.[234]

Other concerns like Google's Street View mapping service blur the line between what should be public and private. Street View uses high resolution cameras to take street-level photographs of buildings and residences. Google has indicated that "Street View only features imagery taken on public property" and "...is no different from what any person can readily capture or see walking down the street."[235] But others fear the easily-accessible, detailed photos, sometimes even into people's homes, are too extreme and people should have a certain degree of anonymity in public places. And if earth-bound cameras not enough, the U.S. Department of Homeland Security has announced that law enforcement agencies will soon be allowed to utilize the nation's most sophisticated spy satellites to monitor American citizens domestically. Privacy advocates fear that the technology will be used irresponsibly, without proper oversight and that it "marks a new era in intelligence gathering."[236]

The real question regarding surveillance cameras and other forms of observation is whether the purported public benefits outweigh the loss of individual rights. From an economic perspective, do the enormous expenditures on the systems translate into real, quantifiable safety gains, or would the money have been better used by putting actual police on the streets? The digitization of surveillance images and infinite storage space raise further questions as to the privacy and safeguarding of the images. Further debate on how far societies are willing to bear the loss of privacy in exchange for the sensation of safety that public surveillance provides is imperative.[237]

---

[234] Judy Dempsey & Katrin Bennhold, *Arrests Spur Surveillance Debate; German Ministers Hold Security Talks Over Foiled Terror Plot*, INT'L HERALD TRIB., Sept. 8, 2007, § News, at 6.
[235] Miguel Helft, *Google Photos Stir a Debate over Privacy*, N.Y. TIMES, May 31, 2007, at C1.
[236] Eric Schmitt, *Liberties Advocates Fear Abuse of Satellite Images*, N.Y. TIMES, Aug 16, 2007, at A16.
[237] See generally, THE ROYAL ACADEMY OF ENGINEERING, DILEMMAS OF PRIVACY AND SURVEILLANCE: CHALLENGES OF TECHNOLOGICAL CHANGE 33-34 (2007), for a more detailed discussion of privacy implications and the use of surveillance.

2. Dataveillance

a. Data mining

Electronic surveillance of personal data, also known as dataveillance, is the result of the huge explosion of the computer revolution and the ever increasing storage and computing capacity worldwide. The public and private sector alike are amassing huge quantities of personal data and use this data to create digital dossiers of individual citizens and consumers. The aggregation of this data is then "mined" for new information and patterns using powerful artificially intelligent computers. The computers scan the data to look for predetermined patterns in the hopes of identifying potential terrorists.[238]

In 1965 the U.S. Government proposed to build a central National Data Center to reduce costs, improve efficiency, and create a single information clearinghouse for federal agencies. By 1968 after much debate and criticism it was clear that the proposal would not be enacted due to the government's inability to guarantee privacy protections,[239] but government agencies proceeded with the digitization of information albeit in the form of thousands of interconnected databases. Arthur Miller wrote a chilling assessment of national databases in 1967 that still resonates today:

> But such a Data Center poses a grave threat to individual freedom and privacy. With its insatiable appetite for information, its inability to forget anything that has been put into it, a central computer might become the heart of a government surveillance system that would lay bare our finances, our associations, or our mental and physical health to government inquisitors or even to casual observers. Computer technology is moving so rapidly that a sharp line between statistical and intelligence systems is bound to be obliterated. Even the most innocuous of centers could provide the "foot in the door" for the development of an individualized computer-based federal snooping system.[240]
>
> ...
>
> Our success or failure in life ultimately may turn on what other people decide to put into our files and on the programmer's ability, or inability, to evaluate, process, and interrelate information. The great bulk of the information likely to find its way into the center will be gathered and processed by relatively unskilled and unimaginative people who lack discrimination and sensitivity. Furthermore, a

---

[238] *See* MARTIN KUHN, FEDERAL DATAVEILLANCE: IMPLICATIONS FOR CONSTITUTIONAL PRIVACY PROTECTIONS (2007) for a more detailed look into data mining operations.

[239] *See* SIMON GARFINKEL, DATABASE NATION 13-14 (2000).

[240] Arthur R. Miller, *The National Data Center and Personal Privacy*, THE ATLANTIC, Nov. 1967, at 53.

> computerized file has a certain indelible quality — adversities cannot be overcome simply by the passage of time.[241]

Miller was accurate in his perception of the consequences of database technology, but what he could not have known about is the sophistication of data mining operations currently being employed around the world.

a. Government Data Mining

One of the consequences of 9/11 was criticism that the government was not able to "connect the dots" to prevent the terrorist attacks.[242] The apparent inability of the government intelligence communities to collect, disseminate, and share their findings has prompted a government-wide effort to update their intelligence systems utilizing the latest technologies. One such attempt by the U.S. Department of Defense's Defense Advances Research Projects Agency (DARPA) was the originally named data mining project Total Information Awareness (TIA). The TIA's goal was to be a broad surveillance system that would utilize databases and data mining techniques to root out terrorist activities.[243] Even though DARPA officials said that they "are not developing a system to profile the American public,"[244] the Big Brother overtones of the program were too strong and the U.S. Senate eventually defunded the program.[245] The TIA's logo (the Illuminati's all-seeing eye), its Latin motto ("*Scientia Est Potentia*" or "Knowledge is Power"), and its leader Admiral John Poindexter, convicted of obstructing justice during the Iran-Contra affair, were additional blunders that led to the program's eventual downfall.[246]

---

[241] *Id.* at 54.

[242] 9/11 COMMISSION, THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES: AUTHORIZED EDITION 416-9.

[243] *See* K. A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 2, at ¶ 71.

[244] Adam Clymer, *AFTEREFFECTS: PRIVACY; Pentagon Surveillance Plan IS Described as Less Invasive*, N.Y. TIMES, May 7, 2003, at A20.

[245] *See* Carl Hulse & Thom Shankler, *Senators Want to Block Spending on Terrorist Initiatives*, N.Y. TIMES, Aug 14, 2003, at A20.

[246] U.S. Senator Ron Wyden et al., Symposium, *Spies, Secrets, and Security: The New Law of Intelligence: Oversight of Intelligence: Law and Policy Efforts to Balance Security, Privacy and Civil Liberties in Post-9/11 America*, 17 STAN. L. & POL'Y REV. 331, 342 (2006).

The demise of the TIA system was seen by some as a coup for privacy rights and weakening government sponsored surveillance, but in reality could have done more harm than good. Instead of having a publicly-known and accountable data mining program where tangible privacy protections and procedures could have been introduced,[247] the data mining operation has been moved to other classified programs and agencies.[248] The Department of Homeland Security's ADVISE program (Analysis, Dissemination, Visualization, Insight and Semantic Enhancement) could be one of the offshoots of the defunct TIA program and is believed to have progressed even further than the former program,[249] prompting an investigation and recommendations to ensure that the DHS is taking the proper measures to comply with privacy laws.[250]

Financial systems have received increased scrutiny since 9/11 with the government's new focus on terrorist financing activities. Through changes in the Patriot Act, the U.S. intelligence agencies have virtual unfettered access to the financial system. Section 361 of the Patriot Act enables the creation of the Financial Crimes Enforcement Network (FinCEN) to monitor "suspicious" activities.[251] Financial institutions are now being enlisted to act as virtual informants of their customers' financial transactions and are required to secretly upload "Suspicious Activity Reports" to the federal government.[252] Former New York Governor Elliot Spitzer found out how thorough the activity reports can be when they led investigators to his involvement in a call-girl sex scandal.[253] In Spitzer's case the transactions were relatively small in sum, leading to the question, at what point does the monitoring of transactional data become burdensome on those wanting to protect the privacy of their purchases. Given the insecurity of electronic payments and credit cards, the only recourse for those concerned with their privacy are

---

[247] *See* Taipale, *supra* note 234, at ¶ 98.
[248] *See* Siobhan Gorman, *NSA's Domestic Spying Grows as Agency Sweeps Up Data*, WALL ST. J., Mar 10, 2008, at A1.
[249] *See* Ellen Nakashima & Alec Klein, *New profiling Program Raises Privacy Concerns*, WASH. POST, Feb. 27, 2007, at D3.
[250] *See* U.S. GAO, DATA MINING: EARLY ATTENTION TO PRIVACY IN DEVELOPING A KEY DHS PROGRAM COULD REDUCE RISKS (2007).
[251] Patriot Act, § 361.
[252] Patriot Act, § 365.
[253] *See* Josh Meyer & Erika Hayasaki, *Bank Transactions Put Focus on Spitzer; Neither the New York Governor nor the Call-Girl Ring He Has Been Linked to Was Specifically Targeted*, L.A. TIMES, Mar. 12, 2008, at A16.

by making cash payments, now monitored by financial institutions. Filing suspicious activity reports run the risk of scrutinizing innocent people engaged in entirely innocent transactions. Further, it was reported in 2006 that SWIFT, a Belgium-based financial transaction record company had secretly and illegally supplied transaction information to U.S. authorities.[254] The privacy invasion caused outrage within the European Union and highlights the difficulty in determining what laws and jurisdictions apply to data and its movement. There is further indication that the U.S. has similar agreements with domestic payment system companies. The CEO of the CHIPS payment system, which handles 8 million transactions totaling over 1.5 trillion dollars per day, is in discussion with U.S. government agents to remove any information sharing obstacles.[255]

Many doubt the effectiveness of data mining efforts. Terrorists are innovative and adaptive; looking for patterns is likely to lead to a high rate of false positives, since it is impossible to know exactly how terrorists will attack. Further, terrorists could defeat the system by merely acting as normal as possible.[256] The 9/11 hijackers were known terrorists to the intelligence agencies, they lived in plain sight, opened bank accounts, obtained drivers licenses, and some were even listed in the phone book. A sophisticated data mining operation would not have been necessary to discover their intentions, just good detective work and efficient information sharing within the intelligence community.[257] Given this, the implementation costs and effects on privacy warrant further debate on the issue. The fact that little is known about many of the programs provides no insight into the scope of data collection and how the information is used or stored. The expansion of data mining and function creep are real threats to privacy and civil liberties. How far should a society go in the name of security?, or better phrased, does large-scale data mining that invades the privacy of millions and possibly even society as a whole balance the risks to civil liberties given the unknown effectiveness of the programs?

---

[254] *See* Walter Pincus, *Watching Finances of Terror Suspects Discussed in 2002*, WASH. POST, July 14, 2006, at A4.
[255] *Id.*
[256] Jeff Jonas & Jim Harper, *Effective Counterterrorism and the Limited Role of Predictive Data Mining*, POLICY ANALYSIS OF THE CATO INST. 8 (2006).
[257] Wyden et al., *supra* note 246, at 348.

b. Private sector espionage

Private companies for years have been collecting consumer data in order to create individual profiles used in customizing and targeting advertising or product offerings. Such information as tax rolls, voting records, purchases, addresses, census data, and marital status allow data aggregators to combine the individual bits of data and other public records into comprehensive consumer profiles. It is common practice to buy and sell this information for any number of commercial interests including advertising and product promotions. Advances in data mining operations now allow analysts to a certain degree of accuracy to predict future buying habits, a virtual goldmine for many companies. But the extent that behavioral advertising impacts an individual's privacy is unclear since the actions of many consumers are contradictory (on one hand, individuals are concerned with privacy, but at the same time knowingly participate in activities that are prejudicial to their privacy, *e.g.* the use of loyalty cards).

Moreover, individuals are voluntarily posting and publicizing a treasure trove of private information on such websites as MySpace and Facebook effectively allowing corporations and anyone else a close and personal glimpse into their lives.[258] It is not necessarily the act of publically posting private information that poses serious privacy dangers, but it is unknown use of this data by third parties. At best, users of social websites are likely ignorant to the privacy risks, or maybe do not care, but regardless, companies should be forthcoming about the uses of personal information and allow the users to make informed decisions.[259]

The collection of information is not always at fault for privacy transgressions, but the lack of adequate data protection is equally decisive. The Identity Theft Recourse Center reported that in 2007 there were 446 data breaches affecting 127,725,343 individuals in

---

[258] Facebook also has dubious ties to the Central Intelligence Agency. *See* Alan Sherry, *But is CIA Spying on Your Private Pages?*, DAILY MAIL (LONDON), Jan. 18, 2008, § IRE, at 18.

[259] Facebook, for example, faced with consumer outcry, was forced to back off a plan to target advertisements based on the information gleaned from an individual's profile or purchases made. *See* Louise Story & Brad Stone, *Facebook Retreats on Online Tracking*, N.Y. TIMES, Nov. 30, 2007, at C1.

the U.S. alone.[260] Identity theft is a growing concern, especially as information and commerce has become increasingly digitalized. The sheer volume of information available and the lax data security requirements facilitate identity thieves, so much so that the purchase price of full U.S. identities (including working credit card numbers, Social Security number, address, date of birth, etc.) has bottomed out at two dollars apiece. EU citizens should be pleased that their full identities sell for thirty dollars each, possibly indicative of the much stronger data protection mandated in the European Union.[261]

But when the government uses private data collectors, privacy problems begin to percolate into a much larger issue. The government use of commercial databases, for example, is dubious since it could be construed as a way for the government to elude privacy laws and legislatively imposed limits that are not applicable to private companies. The U.S. Government Accountability Office (GAO) has recently criticized the Transportation Security Administration (TSA) for just this scenario. A GAO report has said that "the public was not made fully aware of, nor had the opportunity to comment on, the TSA's use of personal information drawn from commercial sources to test the aspects of the Secure Flight Program." [262] The further inability of the U.S. Customs Border Protection Agency to protect air passenger privacy and comply with U.S. privacy laws during the international prescreening process led the European Union to question whether or nor the U.S. could adequately protect their citizens' personal data in conformity with their data directives.[263] When ChoicePoint, U.S. based data collection firm, managed to (possibly illegally) obtain the entire list of Mexico's voters, Mexican government officials were outraged, especially after the U.S. government acknowledgment that they were using the data to trace Mexican citizens.[264]

---

[260] IDENTITY THEFT RESOURCE CENTER, ITRC BREACH REPORT 2007 1 (Feb. 26, 2008).
[261] Jordan Robertson, *Online Crooks Face Tough Competition*, ASSOCIATED PRESS FINANCIAL WIRE, Apr. 8, 2008, § Business News.
[262] U.S. GAO, PRIVACY: KEY CHALLENGES FACING FEDERAL AGENCIES 14 (2007).
[263] Ellen Nakashima, *Customs Breaks Privacy Laws in Data Collection, GAO Says*, WASH. POST, May 16, 2007, at A2.
[264] *See* Oliver Burkeman & Jo Tuckman, *Special Report: How US Paid for Secret Files on Foreign Citizens: Latin Americans Furious in Row Over Selling Personal Data*, GUARDIAN (LONDON), May 5, 2003, § Guardian Home Pages, at 4.

Furthermore, dozens of intelligence organizations, known as "fusion centers," were created in the U.S. after the 9/11 attacks that have broad access to commercial databases ranging from cell phone records, car rental records, financial holdings, insurance claims, and include one database which claims to have records on 98% of Americans. One official associated with the fusion centers commented that "there is never enough information when it comes to terrorism, that's what post-9/11 is all about." The Electronic Privacy Information Center has uncovered agreements between the federal government and the state governments exposing imposed restrictions to state open record and privacy laws.[265] This comes along with a push within state legislatures to enact local legislation specifically exempting the practices of fusion centers from complying with certain privacy laws.[266] However, the secrecy and lack of accountability causes government watchdog groups to question the handling of private information and call on the legislature to regulate the new intelligence centers instead of allowing them carte blanche in domestic espionage.[267]

Immediately following the 9/11 attacks the intelligence agencies stepped up their efforts to recruit the private sector to share information. Some companies feared being uncooperative and unpatriotic voluntarily and without question supplied vast amounts of information to the government. In 2001 the Professional Association of Diving Instructors handed over information on nearly every U.S. citizen who had learned to SCUBA dive in the previous three years, almost two million people.[268] Also, many travel-related companies supplied information, even though they were in violation of their own privacy policies.[269] Only until recently have companies begun to question the information requests.

---

[265] *See* Memorandum of Understanding between the Federal Bureau of Investigation and the Virginia Fusion Center (Feb. 2, 2008) (http://epic.org/privacy/virginia_fusion/MOU.pdf).
[266] *See* Press Release, Electronic Privacy Information Center, EPIC Obtains Documents Revealing Federal Role in State Fusion Center Secrecy (Apr. 11, 2008) (http://epic.org/press/041108.html).
[267] Robert O'Harrow Jr., *Centers Tap into Personal Databases: State Groups Were Formed After 9/11*, WASH. POST, Apr. 2, 2008, at A1.
[268] Eunice Moscoso, Demand *for Data on the Rise; Patriot Act: Businesses Feel Burden of Subpoenas, Court Orders About Patrons*, ATLANTA J.-CONST., Aug. 17, 2003, at E1.
[269] Stephanie Stoughton, *Poll: Firms Relaxed Privacy Rules*, BOSTON GLOBE, Oct 8, 2001, at C4.

Companies are no longer blindly assuming the government has the right to information on their clients, especially when the information is requested without a warrant. The use of National Security Letters[270] has created an environment of mistrust because they allow the government to secretly obtain any information without having to first obtain a warrant. They are issued without judicial review and the only qualification is the "records sought [be] relevant to an authorized investigation to protect against international terrorism."[271] Based on "national security" concerns the recipients of the letters are threatened with prosecution if they publically to acknowledge they have received a letter or attempt to challenge the legality of the searches.[272] Reports are now beginning to surface about the improper and sometimes illegal use of these letters targeting people with no ties to terrorism[273] causing privacy advocates to press for more transparency in their use and to urge for a system of outside checks and balances.[274]

3. Privacy implications of mass surveillance

"As the government surveillance of citizens is made easier, the effect on political speech and anonymity can become oppressive and stunting."[275]

Many proponents of these new threats to privacy refute that they have "nothing to hide," therefore why should they worry if their personal e-mails, grocery purchases, or phone calls are monitored. After all for the average person there is probably nothing too scandalous in their information data for them to be concerned if somebody is watching. But, more accurately the argument should say, "I don't care what happens, as long as it does not happen to me." The "nothing to hide" argument is based on the myth that privacy is solely about hiding a wrong, concealment, and secrecy.[276] Conceptually,

---

[270] National Security Letters are codified under 18 U.S.C. § 2709 (2006).
[271] 18 U.S.C. § 2709(b)(1) (2006).
[272] *See* 18 U.S.C. § 2709(c) (2006).
[273] *See* OFFICE OF THE INSPECTOR GENERAL, U.S. DEP'T OF JUSTICE, A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006 (2008).
[274] Eric Lichtblau, *F.B.I. Says Records Demands Are Curbed*, N.Y. TIMES, Mar. 6, 2008, at A18.
[275] Clyde Wayne Crews Jr., *Human Bar Code: Monitoring Biometric Technologies in a Free Society*, 452 POLICY ANALYSIS OF THE CATO INST. 1 (2002).
[276] *See* Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misconceptions of Privacy*, 44 SAN DIEGO L. REV. 745, 764 (2007).

privacy encompasses much more than secrecy or surveillance. A previously unknown disease found through DNA analysis or future behavioral patterns found through predictive data mining are difficult to hide, since they are not known beforehand. Further, law-abiding citizens using this argument would not want nude photographs taken of them, nor would they give copies of their credit card statements to random strangers. Plainly, the "nothing to hide" argument falls short.

Government surveillance needs to be transparent and regulated with appropriate oversight to prevent totalitarian tendencies. Judicial and legislative approval of surveillance activities is important and strong individual protections should be explicitly outlined with a high degree of enforcement and accountability.

B. Tracking Technologies: Biometrics & RFIDs

1. Biometric technologies, like the dataveillance technologies pose a serious threat to privacy, particularity to the anonymous and autonomous freedom that individuals expect as they live their daily lives. Advances in biometric technologies have blossomed in recent years and while most have accepted and grown accustomed to some of the more familiar forms of biometrics like fingerprint and voice recognition applications, there are a number of less renowned applications that are currently being perfected that will seriously affect autonomy. Of course, ultimately, biometrics can be an excellent tool to increase convenience and security, but proper safeguards and limits will have to be placed on the application of the technology to ensure that an individual's privacy will not be unwittingly violated.

Certainly the introduction of subtle forms of biometric technology like fingerprint readers to combat welfare fraud are sensible applications, but as civil libertarians note "function creep" will incorporate new purposes of biometrics not originally accepted or intended.[277] Social Security Numbers in the United States are a perfect example of function creep. Originally the SSN was intended to only be an identifier for Social Security records, but

[277] John D. Woodward, Jr., *Biometrics: Identifying Law and Policy Concerns*, in BIOMETRICS: PERSONAL IDENTIFICATION IN NETWORKED SOCIETY 396 (Anil Jain, Ruud Bolle, & Sharath Pankanti eds., 2006).

today its use by both private and public sector institutions is widespread. As function creep occurs and governments find new and innovative uses for biometrics the consequences will at minimum be reduced expectations of privacy and in the worst case totalitarian-like surveillance and complete loss of autonomy. Whereas some see biometrics as a way to positively identify people, questions remain to how effective it will really be. Civil liberty groups in England are offering a £1,000 reward for the Prime Minister's fingerprint in an effort to emphasize the insecurity of using such biometrics.[278]

The U.S. Federal Bureau of Investigation has recently released plans to create the world's largest biometric databases storing information about individual's physical characteristics.[279] There are further initiatives to use biometric identifiers in passports, driver's licenses, and other identification documents to aid law enforcement officials in authenticating identity. Further uses of biometrics allow facial recognition software to identify people through camera surveillance images. The 2001 Super Bowl was one of the first public demonstrations of the technology. Law officials matched surveillance camera footage of people entering the stadium to a database of known criminals. The pervasiveness of surveillance camera systems and the equipment of facial recognition software could pose serious losses to privacy as one's anonymity is violated.

It is technology like facial recognition that privacy advocates argue will be used by the state to monitor and record an individual's actions and behavior. The very movements of people could be tracked using this technology as camera surveillance systems are increasingly utilizing facial recognition. The loss of anonymity could be chilling to rights of free speech as people would be less likely to publically protest as abuse by governments to track political dissidents is possible. Facial recognition is often criticized because of it high failure rate to accurately identify people, but this is likely to change as the software become more advanced causing the technology to become reliable.[280]

---

[278] Jamie Doward, *ID Card Rebels Offer £ 1,000 for Brown's Fingerprint*, OBSERVER (ENGLAND), Apr. 6, 2008, at 3.
[279] *See* Ellen Nakashima, *FBI Prepares Vast Database of Biometrics*, WASH. POST, Dec. 22, 2007, at A1.
[280] *See* Crews, *supra* note 275.

2. RFID Chips

Radio frequency identification (RFID) is a new form of machine-to-machine communication using a chip implanted in an item that broadcasts information to a reader that then interprets the "chatter" into beneficial information. The use of RFID chips has revolutionized the logistics industry and has created new, innovative, and efficient means of inventory control and shipping of goods by tagging individual items and shipping crates.[281] Until recently RFID technology was expensive, but with the drastic reduction in price of the individual chips, they are increasingly appearing in a wide variety of consumer goods. The chips range in style from passive, unpowered chips with a limited broadcast signal to chips that are capable of two-way communication with a reader over large distances.

The tracking capabilities of RFID chips are improving drastically and have primarily been used for identifying and tracking animals and livestock,[282] but in 2004 the U.S. Food and Drug Administration approved an RFID enabled chip for human implantation[283] raising fear and speculation from civil rights and privacy groups that RFID chip use in humans could become a human bar code. Some religious groups are even calling the chips the "mark of the beast."[284] The proponents of the chips claim that the chips are safe and secure and could store important medical information that could be used in emergency situations, but recent studies have shown the implanted chips have caused cancer to develop in mice.

RFID technology is revolutionizing the retail inventory system allowing greater supply chain efficiency and inventory control. The chips are being installed into a variety of consumer goods that constantly emit their unique identifier. Some predict that RFID chips will replace the bar code as the price of individual chips become more economical

---

[281] *See generally*, Stephanie Perrin, *RFID and Global Privacy Policy*, in RFID: APPLICATIONS, SECURITY, AND PRIVACY (Simon Garfinkel & Beth Rosenberg eds., 2006).

[282] *See* Holly Foster, *Voluntary or Visionary?*, BEEF TODAY, July 27, 2007, at 1. The use of RFID technologies has not been widely accepted by all members of the beef industry. There are many people concerned over the loss of freedom and privacy associated with the chips' use.

[283] *See* Barnaby J. Feder & Tom Zeller Jr., *Identity Chip Planted Under Skin Approved for Use in Health Care*, N.Y. TIMES, Oct. 14, 2004, at A1.

[284] *See* Ivan Penn, *Invasive IDs?*, ST. PETERSBURG TIMES, July 28, 2007, at D1.

and fuel new convenience technologies, one day allowing a consumer to skip the check-out lines and instead walk through an RFID equipped reader that automatically scans all of the groceries and processes payment by finding the RFID enabled credit card in the consumers purse or wallet. The problem is that the chips broadcast a unique number that by itself is not harmful, but combined with powerful databases that could connect the number with the owner's identity at the point of sale or by other means could enable the owner's movements to be tracked.

Governments are using RFID chips in identity documents to store such information as biometrics. The data on the chips is rarely encrypted and with fairly unsophisticated and publically available technology, an identify thief could "skim" a persons identity documents and all of the information contained on them. The new passport card the U.S. State Department is issuing to frequent travelers to and from Canada and Mexico at land borders is touted as a new convenience technology, but these cards can be read wirelessly from up to twenty feet away, raising concerns over the security of the information contained on the cards.[285]

Location tracking devices like biometrics and RFID chips pose serious threats to privacy and unforeseen negative social consequences. Some liken these technologies to "geoslavery," or the use of location tracking devices resulting in "coercive control over human movement and direction."[286] The restriction of freedom and movement caused by these technologies is much like the restrictions placed on African slaves in the early 19th century. By 2015 it is estimated that over 13 trillion RFID chips will be in use and with companies like IBM patenting RFID skimming systems to be installed in walls and ceilings of public places it is clear that human tracking could soon become a reality.[287]

---

[285] Ellen Nakashima, *Electronic Passports Raise Privacy Issues*, WASH. POST, Jan. 1, 2008, at A6.
[286] William A. Herbert, *OTHER RESEARCH: No Direction Home: Will the Law Keep Up With Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery?*, 2 ISJLP 409 (2006).
[287] Dawn Rae Downtown, *Who's Watching the Watchers?; As Dawn Rae Downtown reports, RFID Tags Embedded in Shopping Carts, Drug Packaging, Even the Walls of Public Washrooms Are Recording Every Step We Take*, GLOBE AND MAIL (CANADA), July 22, 2006, at F6.

Totalitarian governments have long used surveillance and tracking as a means of social control and suppressing political dissidents. If these tracking technologies seem far fetched, one only has to look at the activities of the Chinese government. Since imperial times China has kept detailed records on their citizens, but with the increased mobility and urbanization of the Chinese countryside the Communist government is increasingly turning to technology to keep track of individuals.[288] Shenzhen, China, with the help of American-made surveillance technology, is issuing RFID enabled identification cards that will contain a mass of personal information including work history, personal reproductive history, education background, landlord telephone numbers, religion, police records, and medical information. These cards will allegedly be used as part of a greater surveillance and tracking system including 20,000 biometrically-enhanced surveillance cameras.[289] After the Tiananmen Square killings the U.S. government put export controls on the transfer of crime control technologies to China and is contemplating expanding the ban to sophisticated surveillance equipment.[290] As U.S. Representative Edward Markey notes, "it remains extremely important to have such controls in place so that our country's exports do not enable governments abroad to repress the fundamental freedoms that we cherish here at home."[291] But this statement seems somewhat hypocritical and arrogant -- it is assumes that the government has completely altruistic motives and that the citizens in U.S. need not worry about the domestic use of these technologies. Is it acceptable for the U.S. government to repress fundamental freedoms with these technologies, but not China?

D. Bioethics

Bioethics is generally defined as "the field that addresses the ethical problems posed by modern medicine and biotechnology,"[292] but in the contexts of privacy bioethics centers around bodily integrity and leads to the question: should the human body be the ultimate private space? This question will be especially significant in the coming years as new technologies are refined and put into operation. The U.S. Transportation Security Agency

---

[288] Keith Bradsher, *China Enacting a High-Tech Plan to Track People*, N.Y. TIMES, Aug. 12, 2007, at A1.
[289] *Id.*
[290] Keith Bradsher, *Keeping an Eye on China's Security*, N.Y. TIMES, Jan. 31, 2008, at C1.
[291] *Id.*
[292] Alexander Morgan Capron & Vivki Michel, *Law and Bioethics*, 27 LOY. L. REV. 25, 25 (1993).

is already using new "backscatter" X-ray machines in selected airports that are being called a "virtual strip search" by some advocacy groups because the machines see through people's clothing.[293] Of course, the machines do not pose privacy problems since they are entirely voluntary – for now anyway. Unlocking the human genetic DNA sequence is already well developed and privacy implications of the use of one's genetic make-up are already extensively debated, but a relatively unknown aspect of privacy rights, *neuroprivacy*, is slowly gaining traction as brain reading and monitoring technology is coming to light.

1. Cognitive Liberty

As developments in medical technologies advance, especially those involving the brain, new privacy implications are arising in the area of cognitive liberty. Cognitive liberty is generally defined as the right to freedom of thought.[294] Historically, cognitive liberty has been used to bolster arguments against the prohibition on drug use, but recent advances in brain surveillance technologies have added *neuroprivacy* to the ideals of cognitive liberty.[295] Advocates urge that the brain and one's thoughts are the ultimate private spaces and that no one should be able to intrude, but what was once untouchable is now accessible as new technologies are eroding the previously absolute privacy of one's mind.

Sound technologies utilizing inaudible hypersonic wavelengths have become reality. Devices such as the Audio Spotlight and HyperSonic Sound (HSS) direct inaudible sounds in a tightly focused beam to relay messages seemingly into a person's mind. These devices are already being used in commercial applications to bombard consumers with advertisements and to convey exhibit information at museums.[296] The U.S. Defense Department has adapted HSS to a "non-lethal" weapon that uses the sound waves to debilitate people causing loss of equilibrium, vomiting, and headaches.[297] In Britain, an "anti-teenager" sound device used to disperse crowds of teens called the "Mosquito" has

---

[293] Thomas Frank, *TSA Looks Into Using More Airport Body Scans*, USA TODAY, Oct. 8, 2007, at A3.
[294] *See* Julie Ruiz-Sierra, *Is It Time for a Cognitive Liberty Social Movement?*, 4 J. OF COGNITIVE LIBERTIES 53, 53 (2003).
[295] *See id.* at 58.
[296] *See* David Ho, *FOR YOUR EARS ONLY: Concept of 'Directed' Sound to a Certain Spot Has Started to Gain Traction*, ATLANTA JOURNAL-CONSTITUTION, Feb. 19, 2008, at D1.
[297] *See* Marshall Sella, *The Sound of Things to Come*, N.Y. TIMES, Mar. 23, 2003, § 6 (Magazine), at 34.

been criticized as discriminating and violating the rights of children.[298] These sound devices are not just ordinary acoustical speakers, they penetrate the mind with wave energy that "operates directly on the auditory perceptive centers in the brain."[299] The fear is that this type of technology will lead to far worse intrusions into one's privacy as access and manipulation of one's thoughts and cognitive states will become much more invasive and commonplace.[300]

Technologies affecting cognitive liberty are not just limited to sound penetration. New technologies currently being researched and in some cases adapted for commercial and legal uses have the capacity to reveal certain mental acts like entertaining racist thoughts, lying, or recognizing something.[301] Functional magnetic resonance imaging, or fMRI, measures the blood flow from different parts of the brain and gives the reader a depiction of what parts of the brain are active. For example, scientists can measure the brain's reaction to seeing pictures of recognizable or non-recognizable places. There is further speculation that with fMRI refinement scientists will be able to determine racial prejudices by measuring brain activity by showing pictures of white and black people[302] and other researchers claim that they are able to use fMRI scanners to predict future behavior in their test subjects.[303] The medical implications of this technology are plainly beneficial, but some companies, like No Lie MRI, are marketing this technology as a truth verification system.[304]

Another method, dubbed brain fingerprinting, uses an electroencephalogram to monitor brain responses to selected stimuli by measuring brain wave activity from 300 to 800 milliseconds. Operators of brain fingerprinting devices can determine whether or not a

---

[298] *See* Philippe Naughton, Kids' *Commissioner Calls for Ban on Mosquito, Ultrasonic Anti-teen Device*, TIMES ONLINE, Feb. 12, 2008, http://www.timesonline.co.uk/tol/news/uk/article3356157.ece.
[299] Christian M. Halliburton, *Letting* Katz *Out of the Bag: Cognitive Freedom and Fourth Amendment Fidelity*, 59 HASTINGS L.J. 309, 326 (2007).
[300] *Id.* at 327.
[301] For a general overview of brain-imaging technologies see Henry T. Greely & Judy Illes, *Neuroscience-Based Lie Detection: The Urgent Need for Regulation*, 33 AM. J.L. AND MED. 377 (2007).
[302] Stacey A. Tovino, *Currents in Contemporary Ethics: The Confidentiality and Privacy Implications of Functional Magnetic Resonance Imaging*, 33 J.L. MED. & ETHICS 844, 844 (2005).
[303] William Saletan, *Peering into the Soul*, WASH. POST, Mar. 18, 2007, at B2.
[304] *See* Jason Pontin, *Mind over Matter, With a Machine's Help*, N.Y. TIMES, Aug. 26, 2007, § 3 (Slipstream), at 3.

person has specific information[305] and other potential applications of brain fingerprinting could be to screen people for terrorist inclinations, possibly without their knowledge.[306] The CIA, FBI, Department of Defense, and Secret Service have all expressed interest or use in the technology, although they have noted that real-world applications are still not quite practical – yet.[307] FMRI and brain fingerprinting are only the first step, the technology will eventually improve with the scanners reducing in size, the images having greater resolution, the software becoming more accurate, and the test becoming subtler and more unobtrusive.

The U.S. Department of Homeland Security is reported to be in negotiations with a Russian company to develop a software-based mind reading technology marketed under the name of Semantic Stimuli Response Measurements Technology. The mind reading system measures an individual's mental reaction and response to subliminal messages and will soon be tested as a tool in airport screening.[308] Also, researchers at the University of Buffalo are researching an automated system to monitor biometrics like faces, voices, and other behavioral indicators to determine the likelihood that someone is about to commit a terrorist act.[309]

One's mind is no longer safe from outside intrusion. With the further refinement and as more applications are found for brain imaging and behavior prediction, serious legal implications are evident and limits should be placed on the ability to intrude into the solace of the brain. The U.S. Supreme Court has ruled that in some cases it is in the State's interest to forcefully administer mind altering drugs so that a defendant can participate in a trial.[310] The act of actually committing a crime may soon become the act

---

[305] *See* Halliburton, *supra* note 299, at 322-3.
[306] The Association of the Bar of New York City, *Are Your Thoughts Your Own?: "NEUROPRIVACY" and the Legal Implications of Brain Imaging*, 60 CBA 407, 416 (2005).
[307] *See* U.S. GAO, INVESTIGATIVE TECHNIQUES: FEDERAL AGENCY VIEWS ON THE POTENTIAL APPLICATION OF "BRAIN FINGERPRINTING" (2001).
[308] *See* Sharon Weinberger, *The Weird Russian Mind-Control Research Behind a DHS Contract*, WIRED MAGAZINE, Sept. 2007, http://www.wired.com/politics/security/news/2007/09/mind_reading?currentPage=all.
[309] *See Algorithms; Technology Would Help Detect Terrorists Before They Strike*, BIOTERRORISM WEEK, Nov. 12, 2007, at 12.
[310] *See* Sell v. United States, 539 U.S. 166 (2003).

of thinking about committing a crime. And once at trial for committing a thought crime, your brain could be used against you. But most importantly, intrusions into the mind violate the sacredness of the human ego and autonomy. Do we want to live in society in which even our thoughts are open to public scrutiny?

2. DNA

One of the more controversial uses of biometrics being employed is the use of DNA identification. DNA is considered the most unique and ultimate identifier of a person, and no one except for identical twins share the same DNA sequence.[311] Forensic science has benefited greatly from the use of DNA identification and it has become an important tool to establish guilt or innocence in criminal investigations. The Human Genome Project has advanced medical science greatly by discovering over 1,800 disease causing genes and has fueled new products and live saving cures.[312]

The collection and use of DNA in criminal cases has revolutionized forensic science. One only has to watch the popular television show "CSI" or have followed the O.J. Simpson trial to grasp the importance of DNA evidence within the criminal justice system. DNA can definitively prove guilt and in many cases has proved to exonerate innocent people previously convicted of a crime before the advent of the technology. As with any evidence collected, there are procedures and limitations placed on the investigatory bodies to safeguard Due Process claims and individual rights. The privacy implications surrounding DNA collections revolve around these principles and what constitutes a legitimate search and seizure. In the U.S. DNA evidence collection is murky, and the practice of "surreptitious sampling," the covert collection of DNA samples, is common. For example, the police secretly follow a suspect and wait until he discards a cigarette butt or spits on the street, both actions leave behind a sample of DNA that is later used in court. The Supreme Court has yet to decide on the limits on covert DNA collection, but the Fourth Amendment implications are evident.

---

[311] Anil Jain et al., *Introduction to Biometrics*, in BIOMETRICS: PERSONAL IDENTIFICATION IN NETWORKED SOCIETY 11 (Anil Jain et al. eds., 2006).

[312] Susie Mah, *DNA Deoxyribonucleic Acid, the Blueprint of Life*, TORONTO SUN, Oct. 10, 2007, at 30.

At the heart of the issue is what constitutes a search and to what degree should DNA evidence be allowed, but there are different ways to determine the issue. If the *Katz* doctrine is followed then the reasonable expectation of privacy rule should be analyzed. The court, applying this test, would have to determine whether or not a person has a reasonable expectation of privacy when they shed some of their DNA, something not easily prevented. The other possible scenario is the *California v. Greenwood* decision which held that the Fourth Amendment does not apply to trash left on the curb. Under this scenario, any DNA samples "found" in public settings are admissible, much like "voluntarily" putting garbage out for collection. The problem with this scheme is that it is virtually impossible to avoid leaving DNA in some form, whereas one has a choice in garbage disposal.[313]

Compounding the DNA collection concerns is the emerging tendency to create databases of DNA. The British were the first to implement a mandatory genetic database and reserve the distinction of having the largest catalog of DNA in the world. In the U.K. the police are able to collect and store DNA samples of anyone arrested, regardless of conviction.[314] The U.S. is not far behind Britain with its Combined DNA Identification System (CODIS). Under the U.S. system each state has their own DNA collection legislation, but the F.B.I. has developed a *de facto* national database that consolidates and compares the data from all of the state and federal databases.[315] Critics in Britain warn that the DNA database is ripe for abuse, limit civil liberties, and could be discriminatory. The British database contains 4.3 million profiles with a yearly growth rate of 500,000 samples, by next year it is estimated that 1.5 million samples will be from children.[316] It has been further disclosed that over 150,000 people never convicted of a crime or mistakenly arrested are in the database.[317] And if national databases were not controversial enough, the U.S. F.B.I. is pushing its "Server in the Sky" program to

---

[313] *See* Amy Harmon, *Lawyers Fight DNA Samples Gained on the Sly*, N.Y. TIMES, Apr. 3, 2008, at A1.
[314] *See* Duncan Carling, *Less Privacy Please, We're British: Investigating Crime with DNA in the U.K. and the U.S.*, 31 HASTINGS INT'L COMP. L. REV. 487, 492 (2008).
[315] *Id.* at 491.
[316] *See* Christopher Hope, *One Million Children on DNA Database*, DAILY TELEGRAPH (LONDON), Mar. 21, 2008, at 1.
[317] *See* Angus Macleod, *Police Win Power to Hold DNA of Cleared Suspects*, TIMES (LONDON), May 26, 2006, at 11.

directly link the biometric databases of the U.S., the U.K., Canada, Australia, and New Zealand into one giant international, global database.[318]

The U.S. Supreme Court denied *certiorari* in the case of *United States v. Kincade*[319] which affirmed the state interest in mandatory DNA collection for certain criminal offences. Circuit Judge Reinhardt in the dissenting opinion points out that the CODIS could be expanded to unknown uses and is ripe for abuse. The list of offences qualifying for DNA collection include many innocuous crimes such as "spray painting graffiti on a government building or tearing apart a $ 1 bill in protest..."[320] Reinhart's analysis of the potential dangers posed by DNA databases is chilling:

> The power to assemble a permanent national DNA database of all offenders who have committed any of the crimes listed above has catastrophic potential. If placed in the hands of an administration that chooses to "exalt order at the cost of liberty," the database could be used to repress dissent or, quite literally, to eliminate political opposition. Many of the qualifying offenses in the DNA Act are crimes that involve conduct closely related to the exercise of First Amendment rights to free speech and assembly, such as incitement, civil disorder, and the various forms of "interference" crimes listed above. Other offenses are so vaguely or broadly described that they cover almost any conduct that can be described as unlawful. Even if the list of qualifying offenses in the DNA Act remains static, future governments might use the Act's already wide reach to monitor, intimidate, and incarcerate political opponents and disfavored minorities.[321]

CODIS was initially created to collect only information about convicted sex offenders, but now that the system is in place there is a push to include other types of crimes. Consequently, Judge Reinhardt's fears on the scope of DNA collection have recently become true. The U.S. Government announced that it will now collect DNA information from anyone arrested in connection with a federal crime, including immigrants detained by federal authorities, regardless or innocence or guilt.[322]

---

[318] *See* Sara A. Carter, *Britain's Police Balk at Plug-in to FBI Database; U.S. Aims to Track Criminals Globally by Sharing Biometrics*, WASH. TIMES, Jan. 16, 2008, at A3.
[319] United States v. Kincade, 379 F.3d 813 (2004) (Reinhardt, dissenting).
[320] *Id.* at 846.
[321] *Id.* at 847-8.
[322] *See* Ellen Nakashima & Spencer Hsu, *U.S. to Expand Collection of Crime Suspect's DNA*, WASH. POST, Apr. 17, 2008, at A1.

Fears proliferate that DNA information could be used improperly. Indeed, DNA is more than merely an intricate fingerprint, it contains very personal information on the genetic make-up of a person. In countries like the U.S. where health care is not guaranteed many are refusing to have DNA tests done for fear that their genetic information, especially their predisposition to a disease, might hamper their ability to obtain health insurance in the future, or possibly even employment.[323] Genetic information could lead to discrimination in other areas as well as scientists continue to isolate gene markers that might indicate sexual orientation[324] or even propensity to other types of socially deviant behavior like criminal intent.

[323] *See* Amy Harmon, *Fear of Insurance Leads Many to Shun or Hide DNA Tests*, N.Y. TIMES, Feb. 24, 2008, at A1.
[324] *See* Harold J. Krent, *Of Diaries and Data banks: Use Restrictions under the Fourth Amendment*, 74 TEX. L. REV. 49, 96 (1995).

V. Conclusion

Conceptually, privacy is an integral part of humanity. It forms the basis of interaction and intimacy and gives people the autonomy to develop freely without the scrutiny of outside interference. It is clear that the two main global privacy regimes, the U.S. and Europe, both respect and value the ideal of privacy and seek to protect it by the bestowment of legal rights through constitutional and statutory laws. But there is a constant uncertainty to the degree society is willing to protect privacy, since its nature is particularly ambiguous, relative, and sensitive to societal shifts and new technology. In the post-9/11 world of terrorism and security, privacy is once again at a crossroads and must be recognized as a worthy societal aim, especially noting the importance placed on privacy in free, democratic societies.

"Big Brother" as imaged by George Orwell symbolizes loss of individualism and privacy through a centralized, systematic, and oppressive government power to monitor and control society. Government surveillance is definitely a valid concern, but in some senses Big Brother may be 'us' and not the government. In the world of hidden cameras, Trojan horses and internet espionage, tabloid papers, loyalty cards and commercial data mining, and *many* other forms of surveillance, the real dangers might not be just the government or big business, but instead regular, ordinary people wielding simple devices powered by the internet.

Greater protection of information privacy is paramount as the world settles into the Information Age and beyond. There is an insatiable quest to know everything about everyone empowered by an unprecedented access to information. With advancements in genetic engineering and brain functions, a whole new field of intimate information about people will soon be available.[325] Private sector reforms are needed in countries like the United States to give a larger degree of control and consent of the individual over collected personal information, and further distinction between public and private information needs to be better defined to prevent misuse of data. The collectors of information must invest the necessary infrastructure to safeguard and protect data from

[325] *See* Erwin Chemerinsky, *Rediscovering Brandeis's Right to Privacy*, 45 BRANDEIS L.J. 643, 656 (2007).

outside hacking and unauthorized access, but greater focus should be on creating alternatives that collect and store less personal information. If the overall quantity of data is reduced, then consequences of data breaches will prove to be less severe.

These new technologies are slowly evolving from the development stage to real-world uses, and as this occurs, the privacy regimes will be forced to respond to their acceptable uses. It is clear that both the U.S. and Europe have profound respect for privacy rights, but how far will they be willing to go in the name of privacy?

In the current pro-security climate it is doubtful that the regimes will allow some privacy to trump security concerns, but there is hope. After more than a decade of debate the U.S. Senate recently passed the "Genetic Information Nondiscrimination Act" barring employers and medical providers from discriminating against people based on genetic predispositions,[326] greatly reducing the consequences of privacy invasions into someone's genetic make-up. The European Commission continues to be proactive in its expansion and interpretation of Europe's data directives. They are currently considering a proposal to limit RFID use[327] and another to define and limit what individual information can be collected in relation to one's internet searches.[328]

There are any number of proposed solutions to the privacy debate, but today's arguments boil down to how much information should a third party know about an individual and what is the societal tolerance level for giving up liberty for the sake of security. Governments and other third parties ought to relinquish the notion that they should know everything about everybody and be prepared to bear the costs of knowing less. James Rule affirms that this will entail accepting that "...privacy will often mean less efficiency – less profit, less convenience, more institutional waste, and sometimes even less safety and justice."[329] And as Benjamin Franklin once noted, "those who would give up Essential Liberty to purchase a little Temporary Safety, deserve neither Liberty nor

---

[326] Sean Lengell, *Senate pre-empts DNA-profile Bias; Bill to Protect Job, Health Care*, WASH. TIMES, April 25, 2008, at A3.

[327] *See* European Commission, *Radio Frequency Identification (RFID) in Europe: Steps Towards a Policy Framework*, COM(2007)96 final.

[328] *See Opinion on Data Protection Issues Related to Search Engines*, Article 29 Data Protection Working Group, Doc. No. WP 148 (Apr. 4, 2008).

[329] RULE, *supra* note 214, at 200.

Safety." This idea brings the privacy-security debate into focus and begs the question to what degree should relinquishing privacy rights be degraded to increase being secure? *A balance must be found.*

BIBLIOGRAPHY

Books

9/11 COMMISSION, THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES: AUTHORIZED EDITION.

ELLEN ALDERMAN & CAROLINE KENNEDY, THE RIGHT TO PRIVACY (1995).

Eric Barendt, *Privacy and Freedom of Speech*, in NEW DIMENSIONS IN PRIVACY LAW: INTERNATIONAL AND COMPARATIVE PERSPECTIVES (Andrew T. Kenyon & Megan Richardson eds., 2006).

BLACK'S LAW DICTIONARY 1233 (8th ed. 2004).

Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY (Ferdinand D. Schoeman ed., 1984).

Christopher G.A. Bryant, *Privacy, Privatisation and Self-determination*, in PRIVACY 67 (John B. Young ed., 1978).

FRED H. CATE, PRIVACY IN THE INFORMATION AGE (1997).

THE FEDERALIST NOS. 10, 51 (James Madison).

SIMON GARFINKEL, DATABASE NATION (2000).

DOROTHEE HEISENBERG, NEGOTIATING PRIVACY: THE EUROPEAN UNION, THE UNITED STATES, AND PERSONAL DATA PROTECTION (2005).

IDENTITY THEFT RESOURCE CENTER, ITRC BREACH REPORT 2007 (Feb. 26, 2008).

Anil Jain et al., *Introduction to Biometrics*, in BIOMETRICS: PERSONAL IDENTIFICATION IN NETWORKED SOCIETY (Anil Jain et al. eds., 2006).

MARTIN KUHN, FEDERAL DATAVEILLANCE: IMPLICATIONS FOR CONSTITUTIONAL PRIVACY PROTECTIONS (2007).

JOHN LOCKE, SECOND TREATISE OF GOVERNMENT (1690).

J.S. MILLS, ON LIBERTY (1860).

Brian C. Murchison, *Revisiting the American Action for Public Disclosure of Private Facts*, in NEW DIMENSIONS IN PRIVACY LAW: INTERNATIONAL AND COMPARATIVE PERSPECTIVES (Andrew T. Kenyon & Megan Richardson eds., 2006).

OECD, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (2002).

GEORGE ORWELL, *1984* (Signet Classic 1961) (1949).

THE OXFORD ENGLISH DICTIONARY, VOL. VIII (1978 ed.).

Stephanie Perrin, *RFID and Global Privacy Policy*, in RFID: APPLICATIONS, SECURITY, AND PRIVACY (Simon Garfinkel & Beth Rosenberg eds., 2006).

THE ROYAL ACADEMY OF ENGINEERING, DILEMMAS OF PRIVACY AND SURVEILLANCE: CHALLENGES OF TECHNOLOGICAL CHANGE (2007).

JAMES B. RULE, PRIVACY IN PERIL (2007).

WILLIAM SHAKESPEARE, KING RICHARD THE SECOND.

SURVEILLANCE STUDIES NETWORK, A REPORT ON THE SURVEILLANCE SOCIETY (2006).

Luber C. Velecky, *The Concept of Privacy*, in PRIVACY (John B. Young ed., 1978).

Richard A. Wasserstrom, *Privacy: Some Arguments and Assumptions*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY (Ferdinand D. Schoeman ed., 1984).

Alan F. Westin, *The Origins of Modern Claims to Privacy*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 59 (Ferdinand D. Schoeman ed., 1984).

ALAN F. WESTIN, PRIVACY AND FREEDOM (1967).

John D. Woodward, Jr., *Biometrics: Identifying Law and Policy Concerns*, in BIOMETRICS: PERSONAL IDENTIFICATION IN NETWORKED SOCIETY (Anil Jain, Ruud Bolle, & Sharath Pankanti eds., 2006).

Articles in Journals

The Association of the Bar of New York City, *Are Your Thoughts Your Own?: "NEUROPRIVACY" and the Legal Implications of Brain Imaging*, 60 CBA 407 (2005).

Morey Elizabeth Barnes, *Falling Short of the Mark: The United States Response to the European Union's Data Privacy Directive*, 27 NW. J. INT'L L. & BUS. 171 (2006).

Duncan Carling, *Less Privacy Please, We're British: Investigating Crime with DNA in the U.K. and the U.S.*, 31 HASTINGS INT'L COMP. L. REV. 487 (2008).

Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 174 (1999).

Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 174 (1999).

Erwin Chemerinsky, *Rediscovering Brandeis's Right to Privacy*, 45 BRANDEIS L.J. 643 (2007).

Clyde Wayne Crews Jr., *Human Bar Code: Monitoring Biometric Technologies in a Free Society*, 452 POLICY ANALYSIS OF THE CATO INST. (2002).

Francis S. Chlapowski, Note, *The Constitutional Protection of Informational Privacy*, 71 B.U. L. REV. 133 (1991).

Judith Wagner DeCew, *The Scope of Privacy in Law and Ethics*, 5 LAW AND PHILOSOPHY 145 (1986).

Charles Fried, *Privacy*, 77 YALE L.J. 475 (1968).

Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421 (1980).

Helen L. Gilbert, *Minors' Constitutional Right to Informational Privacy*, 74 U. CHI. L. REV. 1375 (2007).

Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335 (1992).

Henry T. Greely & Judy Illes, *Neuroscience-Based Lie Detection: The Urgent Need for Regulation*, 33 AM. J.L. AND MED. 377 (2007).

Kent Greenawalt, *Privacy and its Legal Protections*, THE HASTINGS CENTER STUDIES: THE FUTURE OF INDIVIDUALISM, Sep. 1974.

Christian M. Halliburton, *Letting* Katz *Out of the Bag: Cognitive Freedom and Fourth Amendment Fidelity*, 59 HASTINGS L.J. 309 (2007).

Jeff Jonas & Jim Harper, *Effective Counterterrorism and the Limited Role of Predictive Data Mining*, POLICY ANALYSIS OF THE CATO INST. (2006).

William A. Herbert, *OTHER RESEARCH: No Direction Home: Will the Law Keep Up With Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery?*, 2 ISJLP 409 (2006).

Michael W. Heydrich, Note, *A Brave New World: Complying With the European Union Directive on Personal Privacy Through the Power of Contract*, 25 BROOKLYN J. INT'L L. 407 (1999).

Jane E. Kirley, *The EU Data Protection and the First Amendment: Why a "Press Exemption" Won't Work*, 80 IOWA L. REV. 639 (1995).

Harold J. Krent, *Of Diaries and Data banks: Use Restrictions under the Fourth Amendment*, 74 TEX. L. REV. 49 (1995).

Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 UTOLTJ 357 (2005).

Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 Berkeley Tech. L.J. 1085 (2002).

Viktor Mayer-Schönberger, *Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing* (Kennedy Sch. of Gov't, Working Paper No. RWP07-022, 2007).

H.J. McCloskey, *Privacy and the Right to Privacy*, 55 PHILOSOPHY 17 (1980).

Alexander Morgan Capron & Vivki Michel, *Law and Bioethics*, 27 LOY. L. REV. 25 (1993).

Glen Negley, *Philosophical Views on the Value of Privacy*, 31 LAW AND CONTEMPORARY PROBLEMS 319 (1966).

Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW AND PHILOSOPHY 559 (1998).

2006 Oliver Wendell Holmes Lecture, *In the Face of Danger: Facial Recognition and the Limits of Law*, 120 HARV. L. REV. 1870 (2007).

Richard A. Posner, *The Economics of Privacy*, 71 THE AM. ECON. REV. 405 (1981).

William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

Sharon H. Rackow, *How the USA Patriot Act Will Permit Governmental Infringement Upon the Privacy of Americans in the Name of "Intelligence" Investigations*, 150 U. PA. L. REV. 1651 (2002).

Joe R. Reidenburg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717 (2001).

Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, 6 PHILOSOPHY AND PUBLIC AFFAIRS 26 (1976).

Jeffrey B. Ritter, Benjamin s. Hayes, & Henry L. Judy, *Emerging Trends in International Privacy Law*, 15 EMMORY INT'L L. REV. 87 (2001).

Julie Ruiz-Sierra, *Is It Time for a Cognitive Liberty Social Movement?*, 4 J. OF COGNITIVE LIBERTIES 53 (2003).

Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misconceptions of Privacy*, 44 SAN DIEGO L. REV. 745 (2007).

Daniel J. Solove, *MODERN STUDIES IN PRIVACY LAW: NOTICE, AUTONOMY AND ENFORCEMENT OF DATA PRIVACY LEGISLATION: Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137 (2002).

John R. Soma et al., *Balancing of Privacy vs. Security: A historical Perspective of the USA PATRIOT Act*, 31 RUTGERS COMPUTER & TECH. L.J. 285 (2005).

David A. Sullivan, *A Bright Line in the Sky? Toward a New Fourth Amendment Search Standard for Advancing Surveillance Technology*, 44 ARIZ. L. REV. 967 (2002).

K. A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 2.

Judith Jarvis Thomson, *The Right to Privacy*, 4 PHILOSOPHY AND PUBLIC AFFAIRS 295 (1975).

Stacey A. Tovino, *Currents in Contemporary Ethics: The Confidentiality and Privacy Implications of Functional Magnetic Resonance Imaging*, 33 J.L. MED. & ETHICS 844 (2005).

Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

Alan F. Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's: Part I: The Current Impact of Surveillance on Privacy*, 66 COL. L. REV. 1003 (1966).

James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004).

Ulrich U. Wuermeling, *Harmonization of European Union Privacy Law*, 14 J. MARSHALL J. COMPUTER & INFO. L. 411 (1996).

U.S. Senator Ron Wyden et al., Symposium, Spies, Secrets, and Security: The New Law of Intelligence: *Oversight of Intelligence: Law and Policy Efforts to Balance Security, Privacy and Civil Liberties in Post-9/11 America*, 17 STAN. L. & POL'Y REV. 331 (2006).

Periodical Publications

Algorithms; Technology Would Help Detect Terrorists Before They Strike, BIOTERRORISM WEEK, Nov. 12, 2007, at 12.

Keith Bradsher, *China Enacting a High-Tech Plan to Track People*, N.Y. TIMES, Aug. 12, 2007, at A1.

Keith Bradsher, *Keeping an Eye on China's Security*, N.Y. TIMES, Jan. 31, 2008, at C1.

Oliver Burkeman & Jo Tuckman, *Special Report: How US Paid for Secret Files on Foreign Citizens: Latin Americans Furious in Row Over Selling Personal Data*, GUARDIAN (LONDON), May 5, 2003, § Guardian Home Pages, at 4.

Sara A. Carter, *Britain's Police Balk at Plug-in to FBI Database; U.S. Aims to Track Criminals Globally by Sharing Biometrics*, WASH. TIMES, Jan. 16, 2008, at A3.

Adam Clymer, *AFTEREFFECTS: PRIVACY; Pentagon Surveillance Plan IS Described as Less Invasive*, N.Y. TIMES, May 7, 2003, at A20.

Helene Cooper, *Passport Files of 3 Candidates Were Pried Into*, N.Y. TIMES, Mar. 22, 2008, at A1.

Justin Davenport, *Tens of Thousands of CCTV Cameras, Yet 80% of Crimes Unsolved*, EVENING STANDARD (LONDON), Sept. 19, 2007.

Judy Dempsey & Katrin Bennhold, *Arrests Spur Surveillance Debate; German Ministers Hold Security Talks Over Foiled Terror Plot*, INT'L HERALD TRIB., Sept. 8, 2007, § News, at 6.

Jamie Doward, *ID Card Rebels Offer £ 1,000 for Brown's Fingerprint*, OBSERVER (ENGLAND), Apr. 6, 2008, at 3.

Dawn Rae Downtown, *Who's Watching the Watchers?; As Dawn Rae Downtown reports, RFID Tags Embedded in Shopping Carts, Drug Packaging, Even the Walls of Public Washrooms Are Recording Every Step We Take*, GLOBE AND MAIL (CANADA), July 22, 2006, at F6.

Gary Emerling, *5,000 Monitoring Cameras Opened to D.C. Police; Rights Group Hit Expansion*, WASH. TIMES, Apr. 9, 2008, at A1.

Barnaby J. Feder & Tom Zeller Jr., *Identity Chip Planted Under Skin Approved for Use in Health Care*, N.Y. TIMES, Oct. 14, 2004, at A1.

Holly Foster, *Voluntary or Visionary?*, BEEF TODAY, July 27, 2007, at 1.

Thomas Frank, *TSA Looks Into Using More Airport Body Scans*, USA TODAY, Oct. 8, 2007, at A3.

Siobhan Gorman, *NSA's Domestic Spying Grows as Agency Sweeps Up Data*, WALL ST. J., Mar 10, 2008, at A1.

Amy Harmon, *Fear of Insurance Leads Many to Shun or Hide DNA Tests*, N.Y. TIMES, Feb. 24, 2008, at A1.

Amy Harmon, *Lawyers Fight DNA Samples Gained on the Sly*, N.Y. TIMES, Apr. 3, 2008, at A1.

Miguel Helft & Andrew Ross Sorkin, *Eyes on Google, Microsoft Bids $44 Billion for Yahoo*, N.Y. TIMES, Feb. 2, 2008, at A1.

Miguel Helft, *Google Photos Stir a Debate over Privacy*, N.Y. TIMES, May 31, 2007, at C1.

David Ho, *FOR YOUR EARS ONLY: Concept of 'Directed' Sound to a Certain Spot Has Started to Gain Traction*, ATLANTA JOURNAL-CONSTITUTION, Feb. 19, 2008, at D1.

Christopher Hope, *One Million Children on DNA Database*, DAILY TELEGRAPH (LONDON), Mar. 21, 2008, at 1.

Carl Hulse & Thom Shankler, *Senators Want to Block Spending on Terrorist Initiatives*, N.Y. TIMES, Aug 14, 2003, at A20.

Kathleen Lucadamo & Pete Donohue, Get *the Cameras Before Terrorists Hit Again*, DAILY NEWS (N.Y.), Oct. 3, 2007, § News, at 10.

Arthur R. Miller, *The National Data Center and Personal Privacy*, THE ATLANTIC, Nov. 1967, at 53.

Peter Morrell, *Watched and Now Listened To, Is Privacy a Thing of the Past?*, THE WESTERN MAIL (WALES), May 24, 2007, § News, at 22.

Abbey Klaassen, *Listen to This: Google Plan Lets Laptops Hear Your TV*, ADVERTISING AGE, June 26, 2006, at 3.

Heather Knight, *Crime Cameras Not Capturing Many Crimes*, S. F. CHRON., Mar. 21, 2008, at A1.

Janet Kornblum, *Always in the Camera's Eye*, USA TODAY, May 27, 2006, at D1.

Sean Lengell, *Senate pre-empts DNA-profile Bias; Bill to Protect Job, Health Care*, WASH. TIMES, April 25, 2008, at A3.

Eric Lichtblau, *F.B.I. Says Records Demands Are Curbed*, N.Y. TIMES, Mar. 6, 2008, at A18.

Angus Macleod, *Police Win Power to Hold DNA of Cleared Suspects*, TIMES (LONDON), May 26, 2006, at 11.

Susie Mah, *DNA Deoxyribonucleic Acid, the Blueprint of Life*, TORONTO SUN, Oct. 10, 2007, at 30.

Josh Meyer & Erika Hayasaki, *Bank Transactions Put Focus on Spitzer; Neither the New York Governor nor the Call-Girl Ring He Has Been Linked to Was Specifically Targeted*, L.A. TIMES, Mar. 12, 2008, at A16.

Eunice Moscoso, Demand *for Data on the Rise; Patriot Act: Businesses Feel Burden of Subpoenas, Court Orders About Patrons*, ATLANTA J.-CONST., Aug. 17, 2003, at E1.

Ellen Nakashima & Dan Eggen, *Former CEO Says U.S. Punished Phone Firm: Quest feared NSA Plan Was Illegal, Filing Says*, WASH. POST, Oct. 13, 2007, at A1.

Ellen Nakashima, *Customs Breaks Privacy Laws in Data Collection, GAO Says*, WASH. POST, May 16, 2007, at A2.

Ellen Nakashima, *Electronic Passports Raise Privacy Issues*, WASH. POST, Jan. 1, 2008, at A6.

Ellen Nakashima, *FBI Prepares Vast Database of Biometrics*, WASH. POST, Dec. 22, 2007, at A1.

Ellen Nakashima & Alec Klein, *New profiling Program Raises Privacy Concerns*, WASH. POST, Feb. 27, 2007, at D3.

Ellen Nakashima & Spencer Hsu, *U.S. to Expand Collection of Crime Suspect's DNA*, WASH. POST, Apr. 17, 2008, at A1.

Robert O'Harrow Jr., *Centers Tap into Personal Databases: State Groups Were Formed After 9/11*, WASH. POST, Apr. 2, 2008, at A1.

On the Record: Scott McNealy, S. F. CHRON., Sept. 14, 2003.

Ivan Penn, *Invasive IDs?*, ST. PETERSBURG TIMES, July 28, 2007, at D1.

Eric Pfanner, *Britain Apologizes for Major Data Breach; 25 Million People May Have Been Affected*, INT'L HERALD TRIB., Nov. 23, 2007, § News, at 5.

Walter Pincus, *Watching Finances of Terror Suspects Discussed in 2002*, WASH. POST, July 14, 2006, at A4.

Jason Pontin, *Mind over Matter, With a Machine's Help*, N.Y. TIMES, Aug. 26, 2007, § 3 (Slipstream), at 3.

Catherine Rampell, *Yahoo Lied About China, Legislators Say*, WASH. POST, Nov. 7, 2007, at D5.

Catherine Rampell & Frank Ahrens, *Google's Ad Reach My Be Unrivaled; FTC Approves DoubleClick Deal*, WASH. POST, Dec. 21, 2007, at D1.

Jordan Robertson, *Online Crooks Face Tough Competition*, ASSOCIATED PRESS FINANCIAL WIRE, Apr. 8, 2008, § Business News.

William Saletan, *Peering into the Soul*, WASH. POST, Mar. 18, 2007, at B2.

Marshall Sella, *The Sound of Things to Come*, N.Y. TIMES, Mar. 23, 2003, § 6 (Magazine), at 34.

Eric Schmitt, *Liberties Advocates Fear Abuse of Satellite Images*, N.Y. TIMES, Aug 16, 2007, at A16.

Alan Sherry, *But is CIA Spying on Your Private Pages?*, DAILY MAIL (LONDON), Jan. 18, 2008, § IRE, at 18.

Louise Story & Brad Stone, *Facebook Retreats on Online Tracking*, N.Y. TIMES, Nov. 30, 2007, at C1.

Stephanie Stoughton, *Poll: Firms Relaxed Privacy Rules*, BOSTON GLOBE, Oct 8, 2001, at C4.

U.S. Case Law

Boyd v. United States, 116 U.S. 616 (1886).

Breard v. City of Alexandria, 341 U.S. 622 (1951).

California v. Ciraolo, 476 U.S. 207 (1986).

California v. Greenwood, 486 U.S. 35 (1988).

Dow Chemical Co. v. United States, 476 U.S. 227 (1986).

Frisby v. Schultz, 487 U.S. 474 (1988).

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

Harris v. United States, 390 U.S. 234 (1968).

Jacobellis v. Ohio, 378 U.S. 184 (1964).

Katz v. United States, 389 U.S. 347 (1967).

Kovacs v. Cooper, 336 U.S. 77 (1949).

Kyllo v. United States, 533 U.S. 27 (2001).

Lawrence v. Texas, 539 U.S. 558 (2003).

Lochner v. New York, 198 U.S. 45 (1905).

Meyers v. Nebraska, 262 U.S. 390 (1923).

New Jersey v. T.L.O., 469 U.S. 325 (1984).

O'Connor v. Ortega, 480 U.S. 709 (1987).

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

Pierce v Society of Sisters, 268 U.S. 510 (1925).

Public Utilities Commission v. Pollak, 343 U.S. 451 (1952).

Roe v. Wade, 410 U.S. 113 (1973).

Sell v. United States, 539 U.S. 166 (2003).

Silverman v. United States, 365 U.S. 505 (1961).

Stanley v. Georgia, 394 U.S. 557 (1969).

The Florida Star v. B. J. F., 491 U.S. 524 (1989).

United States v. Kincade, 379 F.3d 813 (2004) (Reinhardt, dissenting).

United States v. Westinghouse Electric Corp., 638 F.2d 570 (1980).

Vernonia School District v. Acton, 515 U.S. 646 (1995).

Wang Xiaoning v. Yahoo!, No. 07-2151 (N.D. Cal. Apr. 19, 2007) (complaint of tort damage).

Washington v. Glucksberg, 521 U.S. 702 (1997).

Whalen v. Roe, 429 U.S. 589 (1977).

Internet and Electronic Sources

Ann Cavoukian, Information and Privacy Commissioner, Ontario, Canada, Address at the University of Waterloo Computer Science Club: "Privacy by Design": A Crucial Design Principle (Feb. 27, 2007) (video available at http://csclub.uwaterloo.ca/media/Privacy%20by%20Design.html).

Donald Kerr, Principal Deputy Director of National Intelligence, Remarks and Q&A at the 2007 GEOINT Symposium (Oct. 23, 2007) (transcript available at http://www.dni.gov/speeches/20071023_speech.pdf).

Memorandum of Understanding between the Federal Bureau of Investigation and the Virginia Fusion Center (Feb. 2, 2008) (http://epic.org/privacy/virginia_fusion/MOU.pdf).

Philippe Naughton, Kids' *Commissioner Calls for Ban on Mosquito, Ultrasonic Anti-teen Device*, TIMES ONLINE, Feb. 12, 2008, http://www.timesonline.co.uk/tol/news/uk/article3356157.ece.

Press Release, ABI Research, Video Surveillance: A Market Poised for $46 Billion of Explosive Growth (Mar. 18, 2008) (http://www.abiresearch.com/abiprdisplay.jsp?pressid=1081).

Press Release, Electronic Privacy Information Center, EPIC Obtains Documents Revealing Federal Role in State Fusion Center Secrecy (Apr. 11, 2008) (http://epic.org/press/041108.html).

Press Release, Yahoo! Inc., Flickr Adds Video to its Popular Photo-Sharing Community (Apr. 8, 2008) (http://yhoo.client.shareholder.com/press/releasedetail.cfm?ReleaseID=303857).

Sharon Weinberger, *The Weird Russian Mind-Control Research Behind a DHS Contract*, WIRED MAGAZINE, Sept. 2007, http://www.wired.com/politics/security/news/2007/09/mind_reading?currentPage=all.

U.S. DEP'T OF COMMERCE, SAFE HARBOR PRINCIPLES, July 21, 2000, http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm.

EU and International Laws

Charter of Fundamental Rights of the European Union, Dec. 18, 2000, 2000 O.J. (C 364/1).

Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, Europ. T.S. No. 5.

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, Europ. T.S. No. 108.

Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing Personal Data and on the Free Movement of Such Data, October 24, 1995, 1995 O.J. (L281/31).

GATT, General Agreement on Trade in Services.

Universal Declaration of Human Rights, pmbl., G.A. res. 217A (III), U.N. Doc. A/810 (Dec. 12, 1948).

U.S. Laws

THE DECLARATION OF INDEPENDENCE (U.S. 1776).

Cable Communications Policy Act of 1984, 47 U.S.C. § 551.

Children's Online Privacy Act of 1998, 15 U.S.C. §§ 6501-06.

Employee Polygraph Protection Act of 1988,29 U.S.C. §§ 2001-2009.

Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681-1681t.

Federal Communications Act, 47 USCS § 605.

Health Insurance Portability and Accountability Act of 1998, Pub. L. No. 104-191, 110 Stat. 1936.

Privacy Act of 1974, 5 U.S.C. § 552a.

RESTATEMENT (SECOND) OF TORTS (1977).

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

U.S. CONST.

Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2710-2711.

U.S. Reports

U.S. Department of Health, Education and Welfare, *Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and Rights of Citizens* (1973).

U.S. GAO, DATA MINING: EARLY ATTENTION TO PRIVACY IN DEVELOPING A KEY DHS PROGRAM COULD REDUCE RISKS (2007).

U.S. GAO, INVESTIGATIVE TECHNIQUES: FEDERAL AGENCY VIEWS ON THE POTENTIAL APPLICATION OF "BRAIN FINGERPRINTING" (2001).

U.S. GAO, PRIVACY: KEY CHALLENGES FACING FEDERAL AGENCIES (2007).

U.S. OFFICE OF THE INSPECTOR GENERAL, U.S. DEP'T OF JUSTICE, A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006 (2008).