AN UNEQUIVOCAL RIGHT TO PRIVACY: THE BEST PROTECTION AGAINST UNWARRANTED DATA COLLECTION AND PROFILING

Class Term Paper

CSE P590TU

December 10, 2004

Jim Jantos[1]

Ryan Kaneshiro[2]

John Peterson[3]

Ted Zuvich[4]

[1] Primarily responsible for Sections VII and VIII.
[2] Primarily responsible for Section X.
[3] Primarily responsible for Sections I-VI, XI, and XII.
[4] Primarily responsible for Section IX.

I. Introduction

A large segment of the U.S. population is genuinely convinced that computers, by their very nature, prohibitively invade their personal privacy.[1] Clearly, computers dramatically increase one's capabilities to gather and process data about virtually everything relating to others. Today, we live in an era of unprecedented reliance upon information and analysis provided by computers. As computers, software, and data manipulation methodologies grow ever more sophisticated and powerful, data compilation and subsequent analysis of that data has predictably led to profiling of individuals on a large scale.[2] It is this very ability to collect, combine, and analyze data from different databases that worries American citizens. Profiling of individuals is a very real, immediate, and serious threat to the privacy rights and civil liberties of all of us.

Nearly a billion people are now using the Internet as a personal or institutional system of communication.[3] The World Wide Web user base doubles every twelve to eighteen months.[4] This same system that provides humans the capacity to instantly communicate on a planet-wide scale is, at the same time, developing into a tool for the collection of information about average people and their communications. Some users of the Internet want to shield their identities while participating in frank discussions on various sensitive topics, while others fulfill harmless fantasies by role-playing in chat rooms.[5] Others are concerned about unauthorized hacking into computer systems, unauthorized search and seizure issues, unsolicited e-mail, defamation, and secretly creating databases consisting of individual personal information.[6] The nature of the Internet provides a potpourri of challenges to our traditional top down approach to controlling citizen behavior and implementing public policies. It also magnifies the competing interests of commercial business, government, and the privacy concerns of individuals from overreach by government and the private sector. Continued Internet usage will only exacerbate the privacy issue, particularly since there is no formal law

---

[1] Karen Coyle, *A Primer on Internet Privacy*, Computer Professionals for Social Responsibility (1998), p 1, available at www.kcoyle.net/privacyprimer.html.
[2] *Surfer Beware: Personal Privacy and the Internet*, Electronic Privacy Information Center (June, 1997), p. 1, available at www.epic.org/reports/surferbeware.html.
[3] Coyle, supra note 1 at p. 2
[4] William Aspray, *Chasing Moore's Law: Information technology Policy In the United States*, Scitech Publishing, Inc. (2004), p. ix.
[5] Michael Froomkin, *Anonymity and Its Enemies*, Journal of Online Law (1995), par. 29.
[6] Timothy Walton, I*nternet Privacy News*, p. 3, available at www.netatty.com/privacy/privacy.html.

existing in cyberspace. Collection of data and analysis thereof constitute the core of the threat to privacy. Computers plus the Internet produce a multiplier effect in terms of collection and analysis power. This multiplier effect effectively eliminates obscurity through anonymity. Databases are used to manufacture identity profiles on everyone via cross-referencing other databases (Mosaic Theory).[7]

This paper constitutes a cooperative effort between certain computer scientists and lawyers to detail privacy concerns related to Internet data collection and derivative profiling. The paper surveys relevant laws and approaches to privacy, and presents a critical review of present legislative, technological, and self-regulatory attempts to address many of these concerns. The paper concludes with a tailored solution for privacy protection.

II. Privacy: What Is It?

There appears to be a lack of consensus as to what may be considered subject to privacy rules. The Merriam-Webster Online Collegiate Dictionary defines privacy as:

> a) the quality or state of being apart from company or observation: seclusion;
> b) freedom from unauthorized intrusion (one's right to privacy).

Thus, in a sense privacy is the freedom from unauthorized intrusion. Privacy may be defined in such a way that in a cultural context it would apply to certain aspects of a personal nature where one has reasonable expectations of privacy.[8] There are many areas of life that differing cultures choose to consider private. Historically, the people of the United States have associated privacy protection with personal information.[9] We view "snooping" and similar behavior as intrusive and violative of our privacy rights, irrespective of whether or not any personal data has been obtained by those who would engage in such activities.

In the U.S., the right to privacy argument derives from the Fourth Amendment to the U.S. Constitution, which states:

---

[7] Flavio Komives, *We've Got Your Number: An Overview of Legislation and Decisions to Control Use of Social Security Numbers as Personal Identifiers*, 16 Marshall Journal of Computer & Information Law 529, at 535 (1998).
[8] Aspray, supra note 4 at p. 165
[9] Id.

> 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.[10]

While the word "privacy" is not found in the Fourth Amendment, it is obvious how it relates to one's freedom from unauthorized intrusion by the government (as we defined privacy, above). Privacy doctrine has been subsequently interpreted by the U.S. Supreme Court to be the essence of the Bill of Rights, and hence a Constitutional guarantee.[11] Privacy is referred to as the "penumbra right" that grows from and is protected by several of the Constitutional Amendments.[12] Although neither explicitly protected by the Constitution nor specifically spelled out therein, privacy is generally considered a "core value" by most Americans.[13] State constitutions, federal and state statutes, and tort law judicial decisions also provide authority in support of the individual's right to privacy.

At the time the Constitution and the Bill of Rights were written, the Founding Fathers addressed what they believed were the most pressing privacy fears of their day. These fears can be summarized as follows:

1. that the government would search one's home whenever it so desired, confiscating whatever information it deemed desirable for its purposes;
2. that the government would quarter its troops in citizen's home without their consent, effectively placing government spies among the people;[14]
3. that a unified religious majority would impose its doctrines upon the citizenry via effective peer monitoring.

The framers of the Constitution successfully addressed these concerns. Disappointingly, however, they were not able to effectively address the impact of future changes in technology and the concomitant privacy concerns that have gained life as new technologies entrenched their way into American life. As a result of this unfortunate but glaring constitutional drafting failure, we must ask ourselves whether or not the laws

[10] See Fourth Amendment to the U.S. Constitution.
[11] See Schmerber v. Calif., 384 U.S. 757, 779 (1966)
[12] Id. at p. 779.
[13] Lloyd L. Rich, *Right to Privacy in the Workplace in the Information Age*, The Publishing Law Center (1995), p. 1, available at www.public.con/privacy.com/privacy.html.
[14] Id.

protecting the individual's right to privacy are sufficient to protect us from evolving computer related technology.

It would seem that traditional privacy consists of two principles:

a) the freedom from unreasonable surveillance; and

b) the right of the individual to control the access and dissemination of information about himself.[15]

Decisions of the U.S Supreme Court have broadly defined privacy in precisely these ways. The court has recognized "associational privacy," (*NAACP v. Alabama*, 1958); "political privacy" (*Watkins v. United States*, 1957); "right to anonymity in public," (*Talley v. California*, 1960); "reasonable and legitimate expectation of communications privacy," (*Katz v. United States*, 1967); privacy includes personal decisions about sex, marriage, & reproduction, (*Griswold v. Connecticut*, 1966); "individual interest in avoiding disclosure of personal matters, or informational privacy" and "interest in independence in making certain kinds of important decisions," (*Whalen v. Roe*, 1977); the right to be free from unwanted medical attention (*Cruzan v. Missouri Dept. of Health*, 1990); freedom from unwarranted wiretapping, (*Olmstead v. U.S.*, 1928); "freedom from bodily restraint, the right of the individual to contract, to engage in any of the common occupations of life, to acquire useful knowledge, to worship according to the dictates of [one's] own conscience, to marry, establish a home, bring up children, and generally to enjoy those privileges long recognized at common law as essential to the orderly pursuit of happiness" (*Meyer v. Nebraska*, 1923).[16]

A person has privacy in his home because it is possible to close the world out. No one can see or hear you, thus freeing you to do things that if viewable in public would be considered socially unacceptable. Public nudity, for example, is generally unacceptable, but it is common in one's daily household life. Similarly, in most places you can walk down the public streets and not have to worry about someone recording your every movement. Surveillance is nothing more than intentionally collecting information that happens to be about other people. Neither the purpose of the data collection, nor the

[15] See *Whalen v. Roe*, 429 U.S. 589 (1977); *Griswold v. Connecticutt*, 381 U.S. 79 (1965).
[16] *NAACP v. Alabama*, 357 U.S. 449 (1958); *Watkins v. United States*. 354 U.S. 178 (1957); *Talley v. California* 362 U.S. 60 (1960); *Katz v. U.S.*, 389 U.S. 347 (1967); *Olmstead v. U.S.*, 277 U.S. 438 (1928); *Cruzen v. Missouri Dept. Health*, 497 U.S. 261 (1990); See *Whalen* and *Griswold*, supra note 15.

intentions of the data collector ultimately determine what will be done with the data collected in the future. For example, telephone records collected for business accounting purposes are frequently used in police criminal investigations. Thus, purpose and intent of data collection should not be considered in determining a protectible zone of privacy. The fact that surveillance has occurred and information has been collected is what fundamentally matters to the citizen.

Who has access to the information collected about us? What pieces of information are we talking about? A citizen reasonably expects that his medical data, work records, financial records, educational records, military records, shopping habits, and social life are not publicly available. Most of us would consider our privacy violated in those instances where information about our lives is shared with others whom we have not expressly authorized to have it. Governments have the ability to force information sharing because of their positions of power. One might argue that the greatest threat to privacy rights comes from private parties,[17] but private enterprise does not have this similar power.

The primary point about the governmental threat to privacy is that it is the byproduct of self expansion and technological advance. Our federal government is much more dangerous than the business enterprises operating on the World Wide Web. The government has the resources to tap the most advanced technology imaginable. It controls the police, the courts, the laws, and the military forces of the country. Any private sector invention can be legally confiscated by the military (ASPAB) or the national security agencies of the federal government, and any further research thereon stopped. It can force any business enterprise to sell its technology to it. The government already directly controls the most powerful research laboratories in the world, and it helps fund hundreds of major universities through various research grant systems. Consequently, it is the big bear in the baby playpen. Our government's ability to gather information, transmit, store, and analyze such data is staggering. With the advent of Echelon technologies in the late 1950's, it has been able to listen in on to all of our telephone conversations, at will. With the deployment of Tempest, Forward Looking

[17] Anna Shimanek, *Do You Want Milk With Those Cookies? Complying with Safe Harbor Privacy Principles*, 26 Journal of Corporate Law 459, at p. 459 (2001).

InfrarRed, Realtime Residential Power Line Surveillance related, and "talking rock" technologies, agents of the government have been able to wirelessly and remotely surveil computers, radios, televisions, and any other energy using devices. The government employs KH 17, et seq. orbital satellite technology to quietly watch everything that goes on visually on the planet, and then it deploys the FBI, CIA, DIA, NSA, and the NRO to actively analyze such information. With gamma ray technologies, they can see through buildings, underwater, and underground, while maintaining the only known secure communications technology on the planet.[18] The federal government's information storage capabilities are legendary, and with its supercomputers, it has the greatest cross referencing tool for databases in the world. When you couple these amazing powers with what is an essentially unlimited budget (as compared to individual private sector business enterprises) as well as control of the money supply, it is easy to see why a reasoning American might view the government as a bigger threat to his privacy than online businesses. While the effects of corporate and governmental privacy invasion are the same, the corresponding countermeasures necessary to protect one's privacy are rather dissimilar.[19] Information is power. Power and information are inextricably linked. Where the information resides is where the real power lies. In a nutshell, the more others know about you, the more power they have over you. Consequently, electronically computed concentrations of information are inherently and catastrophically dangerous.

III. Explanation of the Constitutional Framework

> The makers of our Constitution understood the need to secure conditions favorable to the pursuit of happiness, and to the protections guaranteed by this are much broader in scope, and include the right to life and an inviolate personality - the right to be left alone - the most comprehensive of rights and the right most valued by civilized men. The principle underlying the Fourth and Fifth Amendments is protection against invasions of the sanctities of a man's home and privacies of life. This is a recognition of the significance of man's spiritual nature, his feelings, and his intellect. Every violation of the right to privacy must be deemed a violation of the Fourth Amendment. Now, as time works, subtler and more far-reaching means of invading privacy will become available to the government. The progress of science in furnishing the government with

[18] See generally John Peterson, *Freedom to Patent: Strategies For Avoiding the National Security Invention Secrecy Trap*, thesis paper for University of Washington L.L.M. Intellectual Property Program, June (2004), available from the author.
[19] CDT Guide to Online Privacy (May 2004), p. 3-4, available at www.cdt.org/privacy/guide/privacy.

> the means of espionage is not likely to stop with wiretapping. Advances in the psychic and related sciences may bring means of exploring beliefs, thoughts and emotions. It does not matter if the target of government intrusion is a confirmed criminal. If the government becomes a lawbreaker it breeds contempt for law. It is also immaterial where the physical connection of the wiretap takes place. No federal official is authorized to commit a crime on behalf of the government.
> (Justice Holmes, Stone, and Brandeis dissenting in *Olmstead v. U.S.*)[20]

Privacy as protected by the federal Constitution is different from tort law privacy protection in several important ways. First, the acts constituting privacy intrusion are dissimilar and second, the methods of protection afforded the citizen are different. Constitutional privacy protects the individual against the intrusive actions of the federal government, whereas, the common law of torts protects the citizen from the actions of other private citizens.[21] Most suits against the federal government, its agents, employees, or contractors ("state action" or under "color of law") include claims based on the Fourth, Fifth, Sixth, or Ninth Amendments. Twenty-four states also have constitutional provisions or statutes that protect the citizen's right to privacy, and some have been construed by the courts to include authority for civil claims. Restrictions imposed by the Fourth Amendment apply to the federal government. The Fourteenth Amendment imposes the restrictions of the Fourth Amendment on the fifty states and their local governments.[22] In contrast, tort common law, state statutes, and federal statutes restrict the actions of private entities.

In *Griswold v. Connecticut*, the U.S. Supreme Court announced the penumbra theory of the right to privacy.[23] Under this theory,

> ...specific guarantees in the Bill of Rights have penumbras, formed by the emanations from those [other Bill of Rights] guarantees that give them substance. Various guarantees create zones of privacy, such as the First Amendment right of association, the Third Amendment prohibition against quartering soldiers in a home, the Fourth Amendment right to be secure in one's person, house, papers, and effects, the Fifth Amendment right not to surrender anything to one's detriment, and the Ninth Amendment right not to deny or disparage any right retained by the people. These cases press for recognition of the penumbral rights of

[20] *Olmstead*, supra note 16.
[21] CDT Guide to Online Privacy, supra note 19, p. 2.
[22] *Katz*, supra note 16.
[23] *Griswold*, supra note 16, at p. 91.

privacy and repose.[24]

The best that can be said for this approach is that it relies heavily on a liberal interpretation of the Ninth Amendment.

In *Katz v. United States* the court shifted its definition of privacy from being place-based to being person-based.[25] The court tried to balance the government interest in protecting society from criminals, with the interest in protecting individuals from government intrusion. It enunciated a so-called two-part "reasonable expectation" test. The first part of the test asked whether or not the individual exhibited a personal expectation of being left alone from the claimed government intrusion. The second part asked the question whether this personal expectation is of the kind that our society is prepared to recognize as reasonable. Hence, we have the rules against unreasonable search and seizure. There is no expectation of privacy for items in plain view, open fields, abandoned buildings, or in public places.[26]

IV. Federal Statutory Privacy Protections

In the U.S., privacy rights have developed in a piecemeal fashion. A patchwork of issue specific and industry related statutes have prevailed over any coherent right to privacy. Included within this hodgepodge of legislation designed to protect citizens are the following acts and statutes:

1. Privacy Act of 1974 (which safeguards the privacy of government collections). 5 U.S.C. Section 552a;
2. Right to Financial Privacy Act of 1978 (which curbs the government's ability to access financial records maintained in financial institutions). 12 U.S.C. Sections 3401, et seq:
3. 1970 Fair Credit Reporting Act (which safeguards the privacy of financial information). 15 USC 1681 et seq;
4. 1986 Electronic Communications Privacy Act (which safeguards the privacy of communications). This was enacted because the federal wiretap statute failed to protect us from modern computer transmission technologies. It is intended to prevent unauthorized surveillance of electronic communications.

[24] Id. at p. 93.
[25] *Katz*, supra note 16.

18 U.S.C. Sections 2510-2521, 2701-2710, 3117, 3121-3126;

5. Telephone Consumer Protection Act of 1991 (which protects telephone privacy). 47 USC 227 et seq.;
6. Health Insurance Portability and Accountability Act of 1996 (which protects the privacy of one's medical records). Public Law 104-191;
7. Video Privacy Protection Act of 1988 (which safeguards the privacy of other personal records). 18 USC §§ 2710-2711;
8. Children's Online Privacy Protection Act of 1998 (which ensure the protection of children's personal information from commercial website misuse). 15 U.S.C. Sections 6501 et seq.;
9. Computer Fraud and Abuse Act of 1994 (which is supposed to contain computer technology abuse in government and banks). 18 U.S.C. Section 1030;
10. Gramm-Leach Bliley Financial Services Modernization Act of 1999 (which requires financial institutions to respect customer privacy, provide security therefor, and maintain confidentiality of customer data, and disclose their privacy policies). 15 U.S.C. Sections 6801 et seq.;
11. USA PATRIOT Act of 2001 (which requires any business that holds customer data to cooperate in giving such data to the government and law enforcement authorities in order to assist in anti-terrorist activities). Pub. Law no. 107-156, 115 Sta. 272;
12. Privacy of Mail (which proscribes access to mail other than the addressee). 39 U.S.C. Section 3623, 1994;
13. Wiretap Statutes (which prevent unauthorized electronic communications interception) 18 U.S.C. Sections 2510 et. seq., 47 U.S.C. Section 605; The Telecommunications Act of 1996 (which sets rules for providers of telecommunications services to protect customer's personal information). Pub. Law 104, section 222, 110 Stat. 56, 1996; and,
14. Computer Matching and Privacy Protection Act of 1988 (which regulates exchange of computerized records among governmental agencies). Pub. Law

[26] *Griswold*, supra note 16, at p. 95.

No. 100-503.

Executive branch agencies also regulate privacy matters. Over the past thirty years, the federal government has engaged in a wide range of privacy initiatives. The Federal Trade Commission has been promulgating privacy regulations for the private sector. So has the White House Office of Management and Budget as well as the U.S. Department of Commerce.[27] In November 1999, the FTC examined online "profiling." Profiling is the practice of compiling information about consumers' preferences and interests primarily via collection of data from tracking consumers' online activities. The resulting profiles are used for a variety of commercial purposes. At present, the FTC supports both self-regulation and further legislation.[28]

V. State and Tort Protection of Privacy

Today, the right to privacy is recognized in practically all fifty states by common case law, state constitutions, or by statute. The federal courts have said that the various states may enact greater privacy protection than that required under federal statutes. Some states have passed laws that appear to protect privacy in such a manner as to clearly include e-mailing.[29] Many state court privacy decisions, however, have traditionally favored employers. It may that the common law of torts will become the battleground for private sector privacy protection decision-making. Of note is The Restatement, Second of Torts, section 652A which states that

> one who invades the right to privacy of another is subject to liability for the resulting harm to the interests of the other. The right to privacy is invaded by the unreasonable intrusion upon the seclusion of another.

Should not The Restatement encompass all invasive activities? There are four common torts that can be cited in the violation of privacy:

a) intrusion upon the plaintiff's seclusion or solitude, or his private affairs;

b) public disclosure of embarrassing private facts about the plaintiff;

c) publicity which places the plaintiff in a false light in the public eye; and,

d) appropriation for the defendant's advantage, of the plaintiff's name or

[27] CDT Guide to Online Privacy, supra note 19, p. 3.
[28] Id. at p. 4.
[29] Id.

likeness.[30]

A serious question remains: to what extent can these common tort remedies of invasion of privacy truly protect us in the digital information age? Defamation too, is generally prohibited, no matter what form it takes. Defamation and disparagement essentially consist of the publication of false and unprivileged statements about someone that are relied upon and bring harm, economic loss, or social ill-repute to the one whop is the object of the statements.

VI. Who Needs or Cares About Privacy?

Some people think that "If I am doing nothing wrong, then I do not need trouble myself with privacy concerns."[31] This is a very naive view of the value of privacy. Hiding illegal activity is only a very small portion of the entire privacy issue. Many of us seek reassurance in the belief that by being insignificant our personal information is not of sufficient interest to be collected, compiled, or correlated with other data.[32] This is a false belief. Digital information is much easier to manipulate, synthesize, analyze, store, and transmit than analog data. It is therefore immeasurably easier to abuse. When one's privacy is violated, without at least mutually agreed upon compensation, one is literally being stolen from. Stolen identity records, for example are typically sold for hundreds of dollars per document. Privacy sensitive information is frequently leaked. How often do we have to deal with telemarketers who obtained information about us via unprotected private data? At the core of this issue is a power struggle. Are we going to maintain the right to control information about our private lives? Everybody who is interested in not being forced into subservient relationships, including criminal ones, by any person or entity that just happens to have the power to collect information that might be harmful to him needs a full blown right to privacy.

Federal information collection systems of many different types raise concerns about the citizen's real privacy rights, especially since the advent of the USA PATRIOT Act.[33] Privacy in federal systems is an important component in protecting against human

---

[30] William Prosser, "Privacy [A legal Analysis]," Calif. Law Rev. 1960, 48: 338-423, at 340.
[31] Privacy Review, *The Ethics of Modern Privacy* (Mar 23, 2004), available at www.jerf.org/writings/communicationsEthics/node9.html.
[32] Jessica Litman, *Information Privacy/Information Property*, 52 Stanford Law Review 1283, at 1285 (2000).
[33] The USA PATRIOT Act (P.L. 107-56).

rights threats. Federal agencies and employees have used citizen information stored in federal systems to carry out political and personal vendettas.[34] Some past abuses include using census data to identify people for internment camps and spying on during WWII, snooping through I.R.S. tax records, and of course Presidential administrations illegally obtaining FBI files on political opponents.[35] We should be concerned about the impact of technology on privacy as well as power. Once the public begins to realize just how much data can be collected and used against it, then it tends to behave more reservedly for the record, rather than freely. Freedom of action and expression get lost because people worry more about how the authorities perceive their behavior, rather than exercising their rights. Government use of surveillance techniques tends to manipulate human behavior. For example, individuals will speak less freely and frankly when they think someone is recording what they say. The idea of free keyboarding in the computer world is about as ludicrous as the idea of free speaking in a world of audio and visual surveillance. Identity theft is a problem in federal information databases. Identity theft occurs because the database is often holding the wrong kind of information and using it improperly.

Why make more federal databases? Our Constitution created a government of narrowly defined and limited enumerated powers. Such a limited government model is the best defense against threats to privacy and other human rights. This is a model of government that the United States has pretty much abandoned since the 1930's. As the federal government adopts more ambitious regulatory programs and agendas, the more its agencies demand personal information from the citizenry. The higher taxes go, the greater become IRS demands for personal and business records. While return to the limited government model might be best as a defense to dangers to privacy, it appears unlikely that that will occur in our lifetimes.

The fundamental threat to civil liberties comes from the growth of governmental power, not the growth of databases. As long as we assume that the federal authorities should be responsible for regulating more and more of our lives, we will not be able to resist their demands for more privacy related data from us. Governments that do more need more tax money to do what they do. It is probably illogical to argue that its taxing

[34] Solveig Singleton, *Privacy issues in Federal Systems: A Constitutional Perspective*, CATO Institute Informational Studies (Mar. 17, 1999), available at www.cato.org/speeches/sp-55031799.html.
[35] Id. at p. 2.

agency will not want to keep closer track of us. As long as government power grows, so will the government databases on the citizenry. Government agencies will attempt to get away with as much invasion of citizen privacy as possible, until angry public opinion causes a change in the law that makes such invasions illegal. This may account for why so many proposed pieces of legislation and piecemeal laws have come into being. Improvements in computer related technology occur so rapidly that changes occur before we realize the capabilities of the previous discoveries. As we gradually catch on to these capabilities, our legal system must catch up with the technology in order to corral the newly surfaced ways of invading our collective privacy. The point is this: the answer to the threat of citizen privacy by powerful government is not the imposition of trifling restrictions on the use of collected data (from which the government will likely exempt itself), but rather to eliminate the power of government to violate our privacy.

VII. EU Data Protection Directive

In contrast to the patchwork of U.S. privacy laws and the uncertain application of U.S. privacy rights to Internet data collection, members of the European Union ("EU")[36] are bound by certain rules governing data protection promulgated under Directive 95/46/EC (the "EU Data Protection Directive").[37] The EU Data Protection Directive was adopted in 1995, and became effective for all EU members on October 25, 1998.[38] The EU Data Protection Directive recognizes privacy as a fundamental right and is designed to uphold individual rights pertaining to the collection and processing of personal data. The EU Privacy Directive has broad application to both traditional paper and electronic personal data, and therefore implicates data gathering and profiling conducted through

[36] As noted on the website http://europa.eu.int, the European Union ("EU") is a family of democratic European countries. The EU presently consists of twenty-five nations including: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, The Netherlands, and the United Kingdom.

[37] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at http://europa.eu.int/comm/internal_market/privacy/law_en.htm (hereinafter "EU Data Protection Directive").

[38] The EU is an intricate organization of institutions shared between EU member states. A principle characteristic of the EU is shared sovereignty, whereby member states delegate certain decision making authority to the EU. With the EU Data Protection Directive, the Council of Ministers enacted policy as recommended by the European Commission. Enacted policy generally preempts inconsistent laws of member states, and the EU Data Protection Directive required member states to amend existing laws to

the Internet. Although many EU member states had pre-existing data protection laws, the EU Data Protection Directive was specifically drafted to provide a unitary approach among EU members.

The omnibus EU Data Protection Directive is a far-reaching approach to privacy and data protection. Based on the interests of the U.S. in the global economy and on the limitations placed on data transfers outside the EU mandated by the directive,[39] the EU omnibus approach raises the question whether the U.S. should follow the EU lead and enact broad legislation along the lines of the EU Data Protection Directive. As discussed in further detail below, the EU Data Protection Directive suffers from many flaws and is not an appropriate approach to address privacy concerns related to online data collection and profiling in the U.S.

A. EU Data Protection Directive – Basic Framework

The EU Data Protection Directive recognizes privacy as a fundamental human right,[40] and the rules set forth by the directive are justified by such right. The EU Data Protection Directive applies to the collection, transmission, and processing of "personal data" within and from the EU. Personal data is defined broadly as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." [41] The EU Data Protection Directive generally takes a top-down approach; privacy rights prohibit certain acts, although the prohibited acts may be subject to one or more exceptions.

Presumably recognizing the existence of legitimate uses of "personal data," the EU Data Protection Directive begins from the position that the processing of personal data is lawful subject to the terms and conditions (i.e. limitations) of the directive.[42] The EU Data Protection Directive requires EU member states to adhere to certain principles

---

comply with the directive by the effective date. Last, the European Court of Justice is empowered to uphold EU law. More detailed information is available at http://europa.eu.int/institutions/index_en.htm.

[39] See notes 59 through 63 and accompanying text.

[40] EU Data Protection Directive, Article 1.

[41] EU Data Protection Directive, Article 2(a).

[42] EU Data Protection Directive, Article 5.

regarding (i) the collection and treatment of personal data;[43] (ii) the processing of personal data;[44] (iii) access and objection by data subjects to personal data;[45] and, (iv) the exportation of personal data outside of the EU. The EU Data Protection Directive requires EU member states to implement legislation consistent with the principles of the directive[46] and the directive mandates enforcement mechanisms for violations of the privacy principles set forth in the directive.[47] The EU Data Protection Directive is limited in scope,[48] which provides for many important uses of personal data beyond the reach of the directive.

With respect to the handling and treatment of personal data, EU member states are required to implement the following policies regarding personal data: (i) personal data must be processed fairly and lawfully; (ii) the data must be collected for specified, explicit and legitimate purposes and not used inconsistently with such purposes; (iii) the data must be adequate, relevant and not excessive in relation to the purposes for which it is collected and processed; (iv) data must be accurate and up-to-date with reasonable steps to erase of rectify inaccurate or incomplete data; and, (v) data must not be kept in a form to permit identification any longer than is necessary for the purposes for which the data were collected or processed.[49]

The EU Data Protection Directive sets forth certain requirements which must be met before personal data may be "processed." Processing of data is defined broadly as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[50] In order to process personal data, one the following requirements must be met: (i) the data subject must unambiguously give consent; (ii) the processing of the data is necessary for the performance of a contract to which the data subject is a party or is a

[43] EU Data Protection Directive, Article 6.
[44] EU Data Protection Directive, Articles 7 and 8.
[45] EU Data Protection Directive, Articles 10, 12 and 14.
[46] EU Data Protection Directive, Article 32.
[47] EU Data Protection Directive, Articles 22 through 24.
[48] EU Data Protection Directive, Article 3.
[49] EU Data Protection Directive, Article 6.
[50] EU Data Protection Directive, Article 2(b).

step at the request of the data subject to enter into the contract; (iii) data processing is necessary for compliance with a legal obligation; (iv) the processing is necessary in order to protect the vital interests of the data subject; or, (v) the "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection."[51]

The EU Data Protection Directive prohibits the processing of "special" data, which includes "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life." [52] However, the prohibition is subject to many exceptions. Special data may be processed if the data subject has given explicit consent to processing, except in the case where applicable law prohibits such consent.[53] Processing of special data is also appropriate when it is necessary for the purposes of carrying out the obligations of the controller related to employment law; to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; to carry out in the course legitimate activities with appropriate guarantees by a non-profit-seeking body with a political, philosophical, religious or trade-union aim; or, when the processing relates to personal data made public by the data subject for the establishment, exercise or defense of a legal claim.[54] Furthermore, special personal data may be processed by health care professionals obligated to secrecy for medical purposes, for purposes related to "substantial public interest," and for criminal and national security purposes under EU member national law provisions that provide "suitable safeguards."[55]

Data subjects under the EU Data Protection Directive are given the rights to access and object to personal data collected and processed. With respect to access, data subjects may confirm whether or not personal data is being processed; to receive a

[51] EU Data Protection Directive, Article 7.
[52] EU Data Protection Directive, Article 8.
[53] EU Data Protection Directive, Article 8(2)(a); the exception raises an interesting issue as to whether it is appropriate for an EU member to deny a data subject the ability to allow processing of special data by prohibiting all instances of consent.
[54] EU Data Protection Directive, Article 8(2)(b) through (e).

communication of the data under processing, the processing method (if automated), and information as to the data's source; and, to rectify, erase, or block the noncompliant processing of data, including notification to third parties to whom noncompliant data has been disclosed.[56] Additionally, data subjects may object to the processing of personal data related to the subject on "compelling legitimate grounds."[57] Furthermore, data subjects may object to certain processing of personal data used for direct marketing purposes.[58]

Of particular importance to countries that are not members of the EU, the EU Data Protection Directive prohibits the export of personal data to a third country unless such country ensures an "adequate level of protection."[59] In effect, the directive attempts to ensure that third countries concur with the fundamental rights recognized by the EU. The prohibition on the transfer of personal data outside of the EU is of particular importance to multinational U.S. companies. In response to the directive, the U.S. Department of Commerce negotiated a "safe harbor" for U.S. companies that was approved by the EU in 2000.[60] Under the safe harbor, a U.S. organization may voluntarily join by agreeing to abide by the following seven safe harbor principles: (1) notice (organizations must notify individuals about the purposes for which they collect and use information); (2) choice (organizations must give individuals the opportunity to opt-out for personal information and opt-in for sensitive information which will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual); (3) onward transfers (to disclose information to a third party, organizations must apply the notice and choice principles); (4) access (individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate); (5) security (organizations must take reasonable precautions to protect personal information); (6) data integrity (personal information must be relevant for the intended use, accurate, complete, and current); and (7) enforcement (independent

[55] EU Data Protection Directive, Article 8(3), (4), and (5).
[56] EU Data Protection Directive, Article 12.
[57] EU Data Protection Directive, Article 14(a).
[58] EU Data Protection Directive, Article 14(b).
[59] EU Data Protection Directive, Article 25.
[60] For background information, see http://www.export.gov/safeharbor/sh_overview.html.

recourse mechanisms and procedures must be available to address individual complaints, with the provision for damages and meaningful sanctions).[61]

If a third country does not provide an "adequate level of protection," the directive provides several additional exceptions to the prohibition of personal data transfer outside of the EU, including: (i) the data subject has given his consent unambiguously to the proposed transfer; (ii) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; (iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; (iv) the transfer is necessary or legally required on public interest grounds, or for legal claims; (v) the transfer is necessary to protect the vital interests of the data subject; or, (vi) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest.[62] Furthermore, an EU member may authorize the transfer of personal data to a non-compliant third country if it can demonstrate the existence and applicability of safeguards to protect the privacy and fundamental rights of individuals, with specific recognition of contractual clauses that protect rights.[63]

In addition to those previously noted, the EU Data Protection Directive is riddled with exceptions. For example, the processing of personal data for historical, statistical or scientific purposes is not prohibited in the presence of appropriate safeguards.[64] Furthermore, historical, statistical, or scientific data may be kept for longer periods with appropriate safeguards.[65] To minimize disruptions in everyday life, personal and household use of data is beyond the scope of the directive.[66] Under certain conditions, churches, trade unions, and other non-profits are permitted to keep sensitive information

[61] Id.
[62] EU Data Protection Directive, Article 26(1).
[63] EU Data Protection Directive, Article 26(2).
[64] EU Data Protection Directive, Article 6(1)(b).
[65] EU Data Protection Directive, Article 6(1)(e).
[66] EU Data Protection Directive, Article 3.

about members.[67] The processing of personal data for journalistic purposes, artistic purposes, and literary expression are also generally exempt from the directive.[68] Most importantly, the scope of the directive does not include the processing of personal data concerning security, defense, and criminal law.[69] EU governments are given the power to adopt legislative measures to restrict the directive to safeguard national security, defense, public security, criminal law, and taxation matters. In essence, an EU member has the option to limit the EU Data Protection Directive exclusively to private interests while excluding the government from the main thrust of the directive.

As applied to data collection and profiling on the Internet, the basic framework of the EU Data Protection Directive provides that, as between private parties, Internet user data may only collected for legitimate purposes; such data may only be processed if the Internet user unambiguously consents; and, the collected data must be current, relevant, accurate, and kept no longer than necessary. Data collected on the Internet within the EU may not be transferred to parties outside of the EU without satisfying certain exceptions. Last, EU member states must provide an enforcement mechanism to uphold the principles of the directive.

B. Criticism of the EU Data Protection Directive

The EU Data Protection Directive has been criticized from many angles. Some of the leading areas of criticism are as follows:

1. Bureaucracy and Complexity

Although the EU Data Protection Directive recognizes the importance of data collection, the directive is based on a top-down approach; all data collection and processing is prohibited unless certain conditions are met. Compliance with the top-down approach imposes heavy costs and inconveniences on EU companies and third country companies attempting to comply.[70]

2. Inconsistent With Other Fundamental Rights

The EU Data Protection Directive has raised concerns as to whether application of the directive will impinge on other fundamental rights. With respect to free speech

[67] EU Data Protection Directive, Article 8(2)(d).
[68] EU Data Protection Directive, Article 9.
[69] EU Data Protection Directive, Article 3.

rights, a literal application of the directive would prohibit the posting of all information on the Internet that identifies an individual.[71] As such, the impact of the directive is overbroad, which implicates freedom of speech. In a recent case, the Swedish Supreme Court reversed the conviction of an individual who posted on the Internet severe criticism of Swedish banks and related bank officials.[72] The conviction was based on Swedish law conforming to the requirements of the EU Data Protection Directive. The court recognized the contradictory requirements of the directive and freedom of speech and broadly interpreted the directive's exception for journalists and authors for free speech purposes.

3. Trade Barrier Concerns

Under the EU Data Transfer Directive, EU companies from EU member states with conforming legislation benefit from the unobstructed flow of personal data within the EU. However, non-EU companies are subject to the general prohibition on data transfer between EU member states and third countries. For example, U.S. multinational companies not participating in the safe harbor are disadvantaged as compared to EU companies and may be subject to substantial penalties for noncompliance. Such disadvantage may be viewed as a significant non-tarriff trade barrier.[73]

4. Unknown Scope of Application

In addition to creating a potential trade barrier, the principles of the directive conceivably apply to a broad range of situations that may implicate non-EU interests to create potential third party liability under the directive. For example, the directive may conceivably apply to an EU consumer surfing the website of a U.S. company and related data collection, even if the U.S. company's server is located within the borders of U.S.[74]

---

[70] See *Privacy and Business Concerns, The EU Data Privacy Directive*, available at http://www.privacilla.org/business/eudirective.html.

[71] See Jacob Palme, *Concerns Regarding the EU Data Directive* (July 17, 2001), available at http://dsv.su.se/jpalme/society/eu-data-directive-revision.html.

[72] See Wendy McAuliffe, *Internet Case Overturns European Data Directive*, SDNet UK (July 18,2001), available at http://www.zdnet.co.uk/print/?TYPE=story&AT=2091511-39020357t-10000013c. Also, see *Swedish Supreme Court on the EU Data Directive*, available at http://dsv.su.se/jpalme/society/swedish-surpreme-court-B293.htm.

[73] See Chet Dembeck, E-Commerce Times (April 7, 2000), *EU Privacy Pact Held Hostage by Powerful Few*, available at http://www.ecommercetimes.com/story/2920.html. See also *The Effects of the European Privacy Directive on Electronic Commerce*, available at http://www.perkinscoie.com/page.cfm?id=309.

[74] See *The Effects of the European Privacy Directive on Electronic Commerce*, available at http://www.perkinscoie.com/page.cfm?id=309.

Furthermore, the directive conceivably applies to all email communications initiated from the EU, since email messages implicate a "data subject" and presumably contain "personal data."[75]

5. Government Exception

The most glaring criticism of the EU Data Protection Directive involves the powers reserved to government.[76] As stated above, the governments of the EU are free to collect and process personal data for purposes of national security, criminal matters, and taxation matters. Viewed broadly, the government exemptions touch upon every conceivable use of personal data. As a result, the EU Data Protection Directive merely applies to the collection and processing of personal data in the private sector, although the principles of the directive are intended to be implemented and enforced by government.

By excluding government, the EU Data Protection Directive fails to recognize the most avaricious collector and user of personal data. Due to a long history of information abuse, governments are generally viewed with suspicion regarding the collection and processing of personal information. The directive recognizes privacy as a fundamental right enforceable against the private sector, but data rights are not enforceable against government, the party charged with enforcement of the directive. The enhanced ability of EU governments to collect, process, and monitor personal data under the directive are contrary to the recognition of privacy as a fundamental right.

C. Should the U.S. Follow the EU Lead?

Although the EU recognition of privacy as a fundamental right is highly commendable, the EU Data Protection Directive suffers from many problems. Application of the directive may contravene other fundamental rights, such as freedom of speech. Additionally, the top-down framework of the directive matches or exceeds the uncertainties and complexities in applying the patchwork of U.S. privacy laws to data collection and processing. Last, the directive falls short by failing to recognize the fundamental right of privacy as applied to government. As such, the directive does not

---

[75] Id.

[76] See generally Solveig Singleton, *Privacy and Human Rights: Comparing the United States to Europe*, (CATO White Papers and Miscellaneous Reports, (December 1, 1999) available at http://www.cato.org/pubs/wtpapers/991201paper.html.

prohibit use of personal data collected on the Internet and related data profiling by the government. The EU Data Protection Directive is not an appropriate framework for the recognition of privacy rights in the U.S.

VIII. Recent Federal Legislative Efforts Addressing Privacy

Although privacy has historically played a role in many U.S. legislative efforts, there has been a flurry of activity in recent years with respect to the recognition of privacy rights pertaining to online data collection and profiling. The heightened activity is partly attributed to suggestions from various Federal Trade Commission ("FTC") reports submitted to Congress.[77] The May 2000 FTC report recommended legislation that would require all consumer-oriented commercial websites that collect personally identifiable information to comply with four widely-accepted fair information collection practices: (1) notice - whereby websites would be required to provide consumers with conspicuous notice of information practices, including what information is collected, how it is collected, how it is used, whether information is disclosed to other entities, and whether other entities are collecting information through the site; (2) choice - whereby websites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided; (3) access - whereby websites would be required to offer consumers reasonable access to the information collected about them, including a reasonable opportunity to review the information and to correct inaccuracies or delete information, and (4) security - whereby websites would be required to take reasonable steps to protect the security of information collected.[78] The FTC reiterated that enforcement through "the use of a reliable mechanism to impose sanctions or noncompliance" remained a "critical ingredient in any governmental or self-regulatory program to ensure privacy online."[79] In July 2000, the FTC issued a report recommending legislation to address online profiling.[80]

A. 106th Congress (1999-2000)

---

[77] See e.g. Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 2000), available at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf, and Federal Trade Commission, *Online Profiling: A Report to Congress, Part 2, Recommendations* (July 2000), available at http://www.ftc.gov/os/2000/07/onlineprofiling.pdf.

[78] Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 2000), available at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

[79] Id.

During the 106th Session of Congress spanning the period of 1999-2000, more than thirty bills introduced in the House and Senate directly addressed Internet privacy rights in some manner.[81] Although significant efforts were spent addressing the topic of Internet privacy during the 106th Congress, none of the major Internet privacy bills were passed and signed into law.[82] Notable Internet privacy legislation during the 106th Congress included: S. 2928 Consumer Internet Privacy Enhancement Act (would require commercial websites to provide specific notice of practices with respect to personally identifiable information and opt-out provisions); S. 2606 Telecommunications and Electronic Commerce Privacy Act (would require opt-in provisions for the collection and disclosure of personally identifiable information with FTC enforcement authority); HR 3321 Electronic Privacy Bill of Rights Act (would require website privacy disclosures, consumer consent, and access to one's own personal data); and, HR 2644 Personal Data Privacy Act (would prohibit government from transferring, selling, or disclosing personal information without consent).[83]

Overall, much of the legislation introduced in the 106th Congress tangentially followed the basic structure of the EU Data Protection Directive and closely followed the guidelines set forth by the FTC regarding notice, consent, access, and security. However, none of the legislative efforts directly addressed the collection and use of online data by government.

B. 107th Congress (2001-2002)

Following the path of the 106th Congress, the 107th Session of Congress considered many Internet privacy bills which addressed both the government's access to and use of information as well as the practices of commercial website operators.[84] Consistent with the results of the 106th Congress, none of the major Internet privacy bills

---

[80] Federal Trade Commission, *Online Profiling: A Report to Congress, Part 2, Recommendations* (July 2000), available at http://www.ftc.gov/os/2000/07/onlineprofiling.pdf.

[81] Marcia S. Smith, *Internet Privacy: An Analysis of Technology and Policy Issues*, CRS Report RL30784 (December 21, 2000), cited in Marcia S. Smith, et al, *Internet: An Overview of Key Technology Policy Issues Affecting Its Use and Growth*, CRS Report 98-67 STM (updated January 31, 2001). Additional information available at http://www.cdt.org/legislation/106th/privacy.

[82] Id. Two legislative matters were signed into law: amendments to the Transportation Appropriations Act (P.L. 106-346) and the Treasury-General Government Appropriations (included in the Consolidated Appropriations Act, P.L. 106-554) which addressed the use of cookies on federal agency Web sites.

[83] Additional information available at http://www.cdt.org/legislation/106th/privacy.

[84] Marcia S. Smith, *Internet Privacy: Overview and Pending Legislation*, CRS Report RL31408 (Updated September 14, 2004).

that addressed the practices of commercial website operators were passed and signed into law. Notable Internet privacy legislation during the 107th Congress that addressed the practices of commercial website operators included: HR 2135 Consumer Privacy Protection Act (would require notice, opt-out provisions for personally identifiable information, opt-in provisions for sensitive personal information, and limits on disclosure by recipients); S. 1055 Privacy Act of 2001 (would limit the sale and marketing of personally identifiable information); S. 2201 Online Personal Privacy Act (comprehensive legislation providing provisions regarding notice, consent, access, security, and enforcement for personally identifiable information); and, HR 4678 Consumer Privacy Protection Act of 2002 (provisions for notice, choice, and access for personally identifiable information).[85]

The 107th Congress did enact legislation that broadened the powers of the federal government with respect to information privacy. In the wake of September 11, 2001, the following four privacy-related laws were enacted by the 107th Congress: The 21st Century Department of Justice Appropriations Authorization Act (P.L. 107-273); the USA PATRIOT Act (P.L. 107-56); The Homeland Security Act (P.L. 107-296); and, the E-Government Act (P.L. 107-347).[86] The USA PATRIOT Act and The Homeland Security Act both broadened the powers of the federal government to monitor Internet activities based on law enforcement and national security justifications. Most notably, the USA PATRIOT Act widely broadens law enforcement's power to monitor Internet activity.[87] The USA PATRIOT Act expands the scope of subpoenas for Internet data, allows ISP's to divulge information under certain conditions, and expands the scope of legal devices and methods used to monitor Internet data by government. However, the USA PATRIOT Act lacks judicial oversight for the use of its procedures. In furtherance of the USA PATRIOT Act, The Homeland Security Act lowers the threshold ("good faith" belief of an emergency involving danger, death, or physical injury) when ISP's may voluntarily disclose information to a government entity.

---

[85] Id. Additional information available at http://www.cdt.org/legislation/107th/privacy.
[86] Id.
[87] Several sections of the USA PATRIOT Act are set to sunset on December 31, 2005. Three bills (S. 1695, S. 1079, and S. 2476) are currently pending to limit or repeal the sunset provision of the USA PATRIOT Act.

On the other hand, The 21st Century Department of Justice Appropriations Authorization Act and E-Government Act represent a recognition of privacy rights for individuals, albeit minimal. The 21st Century Department of Justice Appropriations Authorization Act requires the Department of Justice to report to Congress regarding the use of Internet monitoring systems (Carnivore, DCS 1000, etc.). The E-Government Act places certain restrictions on government privacy practices by providing a set of requirements addressing the privacy of personally identifiable information with respect to government agencies and establishes policies for federal government websites. However, neither The 21st Century Department of Justice Appropriations Authorization Act or the E-Government Act place limitations on the collection of personally identifiable information by the federal government.

C. 108th Congress (2003-2004)

Following tradition, several bills addressing Internet privacy have been introduced in the 108th Congress, although none have been passed and signed into law.[88] HR 69 would require the FTC to prescribe regulations to protect the privacy of personal information collected from and about individuals on the Internet. HR 1636 Consumer Privacy Protection Act of 2003 is similar in form to HR 4678 introduced in the 107th Congress. HR 1636 provides notice, choice, and security provisions for personally identifiable information. Furthermore, HR 1636 provides a self-regulatory "safe harbor" and provides an enforcement mechanism through the FTC. However, HR 1636 covers only commercial entities and specifically excludes the government. Last, S. 745 Privacy Act of 2003 requires commercial entities to provide notice and choice regarding the collection and disclosure of personally identifiable information.

In addition, there are four pending "spyware" bills before the 108th Congress: HR 2929 Safeguard Against Privacy Invasions; HR 4661 the I-SPY Prevention Act; HR 4255 the Computer Software Privacy and Control Act; and S. 2145 the SPY Block Act.[89]

IX. Internet Data Gathering Technology

This section details the technological means used to gather data about an Internet user. This will include a discussion of the methods used to gather data for online

[88] Marcia S. Smith, *Internet Privacy: Overview and Pending Legislation*, CRS Report RL31408 (Updated September 14, 2004). Additional information available at http://www.cdt.org/legislation/108th/privacy.
[89] Id.

profiling, which are primarily cookies and web beacons. Later sections discuss the practice and methods of online profiling.

A. Cookies

A cookie is a small text file placed on a user's computer by a web server when the user accesses a particular website.[90] Its primary purpose is to store small amounts of data relevant to the website. The cookie can also transmit information back to the server that placed it (and usually only the server that placed it), allowing the server to collect information about the person using the website (the host of the cookie).

There are different types of cookies: persistent or permanent cookies remain on a user's computer for varying lengths of time, ranging from hours to years. Session cookies expire when the user exits the browser. These are often used as a convenience method for making a shopping cart or counting the number of unique visitors to a site. They can also be used to simplify some tasks, such as storing logon information so that a user does not have to re-enter a user id and password each time they visit a particular site, for example.

Cookies can be placed on a computer without a user's knowledge, such as when a banner advertisement served by a network advertiser appears on a website. The "Online Profiling" section discusses this in greater detail. For more information on cookies see http://www.cookiecentral.com.

To place a cookie on a given computer, the advertiser's server just has to implement a simple piece of "script" in the HTML documents used to define a web page. See the sidebar for a simple example of Jscript[91] code that could be used to place a cookie on a user's machine.

Users have the ability to accept or decline cookies. Most browsers automatically accept cookies, but users can modify their browser settings to decline cookies, or to issue a warning whenever a website attempts to place a cookie. In many cases, the functionality of a web site depends on the use of cookies, however. A user who declined all cookies may not be able to fully experience the website. A user who wanted a warning before accepting a cookie might be interrupted by a barrage of popup warnings

[90] For a detailed discussion of cookies, see http://www.cookiecentral.com.
[91] Jscript is a Microsoft scripting language used to implement functionality in some web pages. JScript scripts can run only in the presence of an interpreter or "host" such as Internet Explorer.

about cookie placement. Either of these events would seriously disrupt the web-browsing experience.

[SIDEBAR]

The samples below show how to create a cookie and how to retrieve a value from it once it is placed. This sample is taken directly from the Microsoft Visual Studio help documentation.[92]

```
<SCRIPT>
// Create a cookie with the specified name and value.
// The cookie expires at the end of the 20th century.
function SetCookie(sName, sValue)
{
  date = new Date();
  document.cookie = sName + "=" + escape(sValue) + "; expires=" +
date.toGMTString();
}
</SCRIPT>
```

This example retrieves the value of the portion of the **cookie** specified by the *sCookie* parameter.

```
<SCRIPT>
// Retrieve the value of the cookie with the specified name.
function GetCookie(sName)
{
  // cookies are separated by semicolons
  var aCookie = document.cookie.split("; ");
  for (var i=0; i < aCookie.length; i++)
  {
    // a name/value pair (a crumb) is separated by an equal sign
    var aCrumb = aCookie[i].split("=");
```

[92] ms-help://MS.VSCC.2003/MS.MSDNQTR.2003FEB.1033/DHTML/workshop/author/dhtml/reference/properties/cookie.htm.

```
    if (sName == aCrumb[0])
      return unescape(aCrumb[1]);
   }

   // a cookie with the requested name does not exist
   return null;
}
</SCRIPT>
```

Cookies store their data in name-value pairs called “crumbs”. The cookie also has additional parameters that control when it expires, which servers can access it, and whether the cookie is secure (accessible only from a secure environment).

[END SIDEBAR]

B. Web Beacons

“Web beacons” are also known as “web bugs,” “single-pixel gifs,” “clear GIFs” or “1-by-1 GIFs.” Web bugs are tiny graphic image files embedded in a web page. They are generally either the same color as the background on which they are displayed or translucent, so that they are invisible to the naked eye. A web bug is placed in a web page with an HTML tag. The HTML tag is programmed to send information back to its home server, which can belong to the host site, a network advertiser or some other third party. This information can include:

- the IP (Internet Protocol) address of the computer that downloaded the page on which the bug appears,
- the URL (Uniform Resource Locator) of the page on which the web bug appears,
- the URL of the web bug image,
- the time the page containing the web bug was viewed,
- the type of browser that fetched the web bug, and
- the identification number of any cookie on the consumer’s computer previously placed by that server.

Companies use this technique to learn more about how visitors use their sites. The information may be used to target ads to those visitors on other sites. The

clickstream activity may be used to determine future advertising downloaded to your browser.

It is worth noting that cookies and web beacons can also be used in emails.[93] In most cases, a user must opt-in to receive marketing emails from third parties, but there is no guarantee that this has to be the case. When you affirm your selection by clicking a hyperlink in an email or checking a box on a website, your email address gets added to the client's email database.

As part of the commentary included in the May 2000 FTC Report,[94] Richard M. Smith outlined a viable method whereby, in some circumstances, web bugs can also be used to place a cookie on a computer or to synchronize a particular email address with a cookie identification number, making an otherwise anonymous profile personally identifiable.[95]

Web bugs are difficult to block, since they are very similar in coding and appearance to legitimate transparent images used to space text and layout web pages.[96] Web bugs can only be reliably detected by closely examining the source code of a web page and searching in the code for 1-by-1 IMG tags that load images from a server different than the rest of the web page. The only way to disable web bugs is to use a browser (and email system) that allows blocking of third-party images. Not all browsers can do this,[97] although recent changes to Microsoft's Outlook (email) and Internet Explorer can perform this action. Other browsers may also have this capability.

C. Online Profiling

A large portion of online advertising is in the form of "banner ads" placed on web pages. In many cases, web sites do not supply their own banner ads, but instead rely on third-party network advertisers such as DoubleClick or Engage.[98] These network advertising companies can manage and supply advertising for numerous unrelated websites. In the year 2000, DoubleClick (one of the largest Internet advertising

[93] Clear GIFs, http://www.doubleclick.com/us/about_doubleclick/privacy/clear-gifs.asp.
[94] Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 2000), available at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.
[95] http://www.ftc.gov/bcp/workshops/profiling/comments/rsmith.htm.
[96] http://www.ftc.gov/bcp/workshops/profiling/comments/wbfaq.pdf.
[97] http://news.com.com/2100-1023-960509.html.

networks) served an average of 1.5 billion ads per day to websites.[99] In 2003, they served an average of 1.8 billion ads per day.[100]

Advertising networks do not merely supply banner ads; they also gather data about the consumers who view their ads. The primary technologies used to enable this are cookies and web bugs, as discussed above. The ad networks can compile the following types of information about any activity that takes place on the computer,[101] including:

- pages viewed,
- links clicked and other actions taken,
- query terms entered into search engines,
- purchases,
- "click-through" responses to advertisements, and
- standard information that the browser sends to every website visited, including IP address, browser type and language, access times, and referring Web site addresses.

All of this information can be obtained without the user having to click on even a single ad.

The information gathered in this fashion is usually anonymous. In most cases, the profile is linked to an identification number in a persistent cookie left by the network advertiser on the user's computer, as opposed to being linked to the name of a specific person. This is non-PII, or "non-personally identifiable information."

There are ways to link the profiles derived from tracking web activities to personally identifiable information, however. The main methods whereby an advertising network can link non-PII to PII are as follows: first, the website to whom personal information (through a form or application filled out by the user) is provided may, in

---

[98] Other ad networks include: Ad4Ever; AdCentric Online; Ad Dynamix; AdSolution; Avenue A; BlueStreak; BridgeTrack; DoubleClick; efluxa; Enliven; Flycast; i33; Mediaplex; PlanetActive; Pointroll; Profero; Qksrv; RealMedia; RedAgency; TangoZebra; TargetGraph; TrackStar; Travelworm; and Unicast.

[99] Federal Trade Commission, *Online Profiling: A Report to Congress* (2000), available at http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf.

[100] The Year in Online Advertising, March 2004, available at http://www.doubleclick.com//us/knowledge_central/documents/trend_reports/dc_2003yearinonline_0403.pdf.

[101] http://privacy.msn.com/, see section "Collection of Your Personal Information."

turn, provide that information to the network advertiser; and second, depending upon how the personal information is retrieved and processed by the website, the personally identifying information may be incorporated into a URL string that is automatically transmitted to the network advertiser through its cookie. This includes the method of using web beacons to link PII to a profile, as discussed in the comments by Richard M. Smith.[102]

A previously anonymous profile can also be linked to personally identifiable information in other ways. For example, a network advertising company could operate its own Web site at which consumers are asked to provide personal information. When consumers do so, their personal information could be linked to the identification number of the cookie placed on their computer by that company, thereby making all of the data collected through that cookie personally identifiable.

As a specific example of this type of linkage, the DoubleClick privacy policy[103] points out that DoubleClick may user voluntarily supplied personal information in order to facilitate the delivery of goods, services, or information, and that DoubleClick may use this PII for "aggregate analysis." It is unclear whether DoubleClick will link PII with previously collected non-PII while performing this analysis.

D. Data Mining and Analysis

Once collected, the network advertiser (or another party) can analyze the profile data and may combine it with data from third-party sources, data on the consumer's offline purchases, or information collected directly from the consumer via surveys and registration forms. All of this data will be stored in a large database, which allows the advertising network to use data mining techniques to make inferences and conclusions about the consumer's preferences and interests. Data mining was originally a term referring to overusing data to draw invalid inferences,[104] but today refers to the process of executing complex queries on large, sometimes seemingly unrelated databases to draw useful summaries of data. In this case, the data miners are interested in producing profiles of people, and analyzing activity and deducing patterns in the information.

---

[102] See note 95 supra.
[103] DART and Privacy, http://www.doubleclick.com/us/about_doubleclick/privacy/Internet-ads/dart.asp.
[104] http://www-db.stanford.edu/~ullman/mining/overview.pdf.

The result of the data gathering and analysis is an extremely detailed profile that can be used to predict the individual consumer's tastes, needs, and purchasing habits. Because the network advertiser can track a consumer on any web site served by the company, they can collect data across unrelated sites on the web. The tracking can also occur over extended periods of time, thanks to persistent cookies. The advertising companies' computers can then use sophisticated algorithms to analyze this profile and decide how to deliver ads directly targeted to the consumer's specific interests, or even things that they might be interested in. This is similar to the practice (found on most bookselling websites) of telling you that "people that bought (the book you just purchased) also bought Jane Smith's Poem Collection."

The potential impact of this extensive and sustained profiling is staggering. Given the current political climate and the behavior of the media, imagine the frenzy in 20-30 years when a profile analysis reveals that a candidate in a tight Senatorial election web-surfed to www.playboy.com a few times when he was a young adult. Or suppose that detailed profile analysis by the government discovers that 10% of the people who have web-surfed looking for information on terrorism, tax evasion, bomb technology, embedded programming, pornography, and blue cheese pasta recipes are in fact terrorists. There is also the potential for spurious data entering a profile.[105]

E. How Online Profiling Works

"Online Profiling: A Report to Congress"[106] provides an excellent anecdotal illustration of how online profiling works. In slightly more technical terms, the process is as follows:

1. When the user first enters a site, the browser automatically sends some information to the server so that the site can communicate with the user's computer. Information such as browser type, browser version, hardware version, operating system, and the language used by the computer, as well as the computer's IP address.

[105] For example, while writing this report and searching for information on DoubleClick, I accidentally went to www.directclick.com. Don't make the same mistake.
[106] See note 99 supra.

2. The server responds by sending back appropriate HTML code for the requested page. A user may get a different layout when requesting a web page from a wireless PDA versus a desktop PC, for example.
3. Embedded in the HTML code that the user receives is an invisible link to the online profiling site. The browser automatically sends (gets triggered) another HTTP request which identifies the browser type and operating system; the language(s) accepted by the browser; and the address of the referring Web page.
4. Based on this information, the online profiler places a banner ad in the space at the top of the page. The ad will appear as an integral part of the page.
5. The online profiler can now place a cookie with a unique ID number on the user's computer, if there isn't one there already.
6. As the user moves around between web sites serviced by the online profiler (network advertiser), the network advertiser can build a profile of the user. Each time the user visits a new site or clicks a link serviced by the particular advertiser, more information gets transmitted, which helps to build the detailed profile. In addition, the online profiler can associate any search terms that the user enters on linked sites, and add those terms to the developing profile.
7. The network advertiser analyzes the collected profile information and makes some decisions about what ads to serve to the user the next time they surf the Web. As an example, if a user searches for golf clubs on a sporting goods site and Scotland on a travel site, they might get an ad for a golfing vacation package in Scotland the next time they surf the web.

F. Profile Access

Users have a limited ability to edit their online profiles. For example, a user of MSN may edit the information in their Microsoft Passport, change billing information, or edit information in their MSN public profile [12]. Note, however, that a user cannot edit their profile to remove the fact that someone using their computer visited the subversive and controversial www.gamedev.net website.

G. Visibility

In most cases, online profiling activity is invisible to the consumer. The presence and identity of a network advertiser on a particular site, the placement of a cookie on the consumer's computer, the tracking of the consumer's movements, and the targeting of ads are simply invisible in most cases. There are essentially only two viable ways to discover that online profiling is taking place: the user can either set the browser to warn about cookies, or review the privacy policy of every website visited. Unfortunately, very few people have even heard of (Internet) cookies, and even fewer have a basic understanding of what one does.[107] Turning cookies off is difficult,[108] and most people would not know that they could do so in any case. In many cases even reviewing a website's privacy policy will not help you, as a significant number of websites do not disclose the fact that they use or allow cookies. The May 2000 FTC Report discusses these statistics in detail, but the basic finding is that most of the sites surveyed allowed third-party cookies, but not all of them disclosed this fact.[109]

Reviewing all the privacy policies on every web site visited is impossible, in practical terms. In a typical browsing session, a user might visit dozens of apparently unrelated sites. Web sites do not typically provide prominent placement for their privacy policy, as discussed in the findings of the May 2000 FTC Report. Such documents can also easily amount to 32 pages of single-spaced tortured legalese, which you cannot expect a person to read, digest, and understand in a limited amount of time. So the typical response is "I just need to get on with my surfing." In many cases, the user agrees to a privacy policy that he or she has not read (and does not have time to read), which could almost literally contain anything. It also may be difficult to find. Perhaps the link is in very tiny type at the bottom of an obscure sub-page, instead of featured prominently on the site's home-page. The Network Advertising Initiative self-regulatory principles[110]

---

[107] Business Week/Harris Poll: A Growing Threat, available at http://www.businessweek.com/2000/00_12/b3673010.htm.

[108] As an example, in Internet Explorer, you need to open the Tools menu, select Internet Options, select the Privacy tab of the dialog that opens up, and then either set the security slider to an appropriate level that will be applied to all websites, or manually adjust the settings for each type of Internet Zone using the Advanced settings option.

[109] See table 15B of the May 2000 FTC Report, supra note 90. Of the websites where third parties can place cookies, only 22% of the sites disclosed this fact.

[110] http://www.networkadvertising.org/aboutnai_principles.asp.

state that a network advertiser's customers should post a privacy policy that clearly and conspicuously discusses the use of profiling data, but this rarely occurs.

H. Invasive Profiling

In addition to "passive" online profiling through clickstream analysis and the gathering of data input into ordering forms, etc., there exists the possibility of more invasive profiling using spyware and adware. Spyware is software that collects information about the use of the computer and periodically relays that information back to a collection center. Alternatively, also refers to software that can record a person's keystrokes and make it available to another party. It is certainly possible to make spyware that can silently deploy onto a target computer via email.[111]

Adware is advertising supported software[112]. The software can usually be downloaded free from the web, but it contains banner advertisements that create revenue for the company. Adware will usually install components on the computer that will send marketing information whenever the user is online. Adware usually contains a disclosure telling you that they will be using your information.

A recently reported case involving MyFreeCursors.com illustrates some of the problems with adware.[113] In this case, the website MyFreeCursors.com advertised a "free" mouse cursor available for download, with the plea to "Show your support for our troops by downloading our free cursors!" The catch was that by downloading the cursor software, users also agreed to install a number of other programs made by the company, including a product called "KeenValue." This product allowed eUniverse (the parent company of MyFreeCursors.com) to collect information such as:

- Websites/pages viewed,
- The amount of time spent on some websites,
- Response to advertisements displayed,
- Standard web log information (IP address, system settings, software installed on your computer, first and last name, country, five digit zip code), and
- Usage characteristics and preferences.

---

[111] William Aspray, Chasing Moore's Law: Information technology Policy In the United States, Scitech Publishing, Inc. (2004), p. 198.
[112] http://www.spywareonline.org/adware.html.
[113] Patriotism? No, Just More Popups," http://www.msnbc.msn.com/id/3078630.

This amounts to a very detailed, very specific online profile. Notice the similarity? The difference in this case (as opposed the data gathering conducted by ad networks) is that the KeenValue software allowed eUniverse to track every website viewed on the computer, not just the ones linked to their ad network.

Despite the apparent invasive gathering of information, Anthony Porter of SpywareGuide.com agreed with the assertion that KeenValue was not (quite) spyware – it was merely very invasive adware.[114] Other adware programs such as Gator and eZula operate in a similar fashion.

EUniverse spokesman Todd Smith said that the practice of linking the adware program to the plea for web users to "support our troops" was a common practice in Internet advertising.[115] The most common Internet model today provides free content, most often subsidized by advertising.

X. Privacy through Self Regulation

Whereas, browsing though the shelves at a public library can be performed anonymously, browsing the World Wide Web leaves behind a surprising amount of information about the user. The privacy threats created by this information trail are compounded by the fact that data can be kept in electronic storage for extended periods of time and retrieved at a moment's notice. Is industry self-regulation a viable option for maintaining privacy? This chapter will examine the limitations of purely technical tools designed to allow users to control how their personal information is disseminated, and critique organizational approaches with respect to how well they disclose privacy policies to the consumer.

A. Web Anonymizers

Website data collection can be classified into two areas: passive or active. Passive data collection is invisible to the user and is automatically sent by web browsers when navigating through a website. Each time a link is clicked, a client will send a request to the remote server for the desired resource. By looking at the header information in a web request, a remote web server can retrieve the user's IP address, browser type, and the page the user was referred from. Cookies and web beacons are

[114] Id.
[115] Id.

other forms of passive data collection that can be used to uniquely identify visitors and track their movements between websites. In active data collection, the user explicitly provides data to the website. Examples of this include filling out registration forms to obtain access to restricted content, entering shipping information to complete an order, or submitting personal preferences to customize the browsing experience.

A web anonymizer is an intermediary that sits between a client and a remote site and intercepts web traffic passing between the two. Instead of sending requests directly to a remote site, a user first send them to the anonymizer which repackages the requests and then forwards them on to the remote site. From the remote site's point of view, it is communicating with the anonymizer, not the user. The web page returned by the remote site will contain hyperlinks to other servers. Before passing the page back to the client, an anonymizer will automatically 'scrub' the links so that they refer to the anonymizer rather than the original source. When a user clicks on a hyperlink in the scrubbed page, the request is first sent to the anonymizer.

There are several variations on the theme that increase privacy. Secure communication schemes such as SSL can be added between the client and the intermediary to prevent an eavesdropper from intercepting data sent between the user and the anonymizer. A chain of anonymizers can also be used to forward requests along. With this technique, the original requester cannot be determined unless all anonymizers along the path are compromised.[116]

Unfortunately, an anonymizer is not a perfect solution. Web browsers are complicated pieces of software and as a result there are several ways that an anonymizer can be confounded. The pages a browser needs to render not only contain static hyperlinks but also pieces of code written in JavaScript that needs to be interpreted by the browser. JavaScript can be used to dynamically insert links in a remote site on a web page. It is a difficult task for an anonymizer's page scrubber to perform a shallow syntactic analysis of JavaScript code and remove potential hazards in a timely fashion.[117] Ad-hoc rule-based approaches that attempt to recognize potentially malicious JavaScript

[116] Proxychain is an example of such an anonymizer, available at http://www.proxychain.com/proxychain.
[117] David Martin and Andrew Schulman, *Deanonymizing Users of the SafeWeb Anonymizing Service*, in Proceedings of the 11th USENIX Security Symposium (2002), p. 129, available at http://www.cs.uml.edu/~dm/pubs/safeweb-usenix-homepageversion.pdf.

statements are akin to plugging leaks in a crumbling dam with one's fingers. More systematic techniques require a deeper analysis of the code but also degrade the page rendering speed. Because of this, users are forced to choose between anonymizers that support JavaScript, but are slower to render, or anonymizers that require the disabling of JavaScript and may result in incorrectly rendered or broken web pages.

Another way to bypass the protection afforded by an anonymizer is through third party viewer applications. When certain types of media are opened, the browser will transfer control to the viewer. An anonymizer only has control over the HTML that is sent to the browser and can do nothing about viewers that wish the transfer of personal information. For example, clicking on a PDF link will display the document in a browser window, but control has actually been transferred to Adobe Acrobat. This can result in a situation where a user is under the mistaken impression that he or she is protected when in fact, a viewer is transferring personal information from under the anonymizer's nose.

Anonymizers are useful for hiding passive information, but a user who provides active information by filling out web forms circumvents the privacy protection. In certain situations, providing active information is unavoidable in order to retrieve content. Many news websites such as the New York Times require registration in order to view articles. Bugmenot.com solves this problem by providing a publicly accessible database that contains a set of names and passwords for sites that require free registration.[118] A user can register with a website and then send the account information to bugmenot.com so others can use the login information in lieu of registering. Since many users login with the same account, usage information gathered by the website is lost in the shuffle. However, the ability to blend-in is a hindrance when trying to establish a persistent profile. Building a user profile is crucial for crafting personalized pages and in maintaining a presence in virtual communities such as online message boards. The Lucent Personal Web Assistant (LPWA) tackles the problem of maintaining a profile while remaining anonymous, by providing an alias email address that the user can provide to a remote site during registration.[119] The remote site only has knowledge

[118] Frequently Asked Questions - BugMeNot.com, available at http://bugmenot.com/faq.php.
[119] Eran Gabber and Phillip Gibbons and Yossi Matias and Alain Mayer, *How to Make Personalized Web Browsing Simple, Secure, and Anonymous*, in Proceedings of the First International Conference on

of a user's alias account information; LPWA automatically forwards mail onto the user's real address. LPWA can be setup to use different aliases for each website with which a user might to register with to thwart any attempts at data fusion across sites.

Despite the use of web anonymizers to maintain privacy, they are not sufficient in and of themselves when considering the active information required to complete an e-commerce transaction. To complete a transaction for a physical good, a user needs to provide payment information and an address in order to receive his product. Concerned users can avoid electronic payment by using money orders or cashier's checks, but at the cost of delayed shipping. Anonymizing a delivery address is a bigger problem. P.O. Boxes can be used, but shipping companies such as UPS and FedEx will not deliver to them. Purchasing plane tickets online without providing a real name and contact information is nearly impossible, given post-9/11 security protocols. Completely anonymizing an e-commerce transaction is a difficult task at best, and it is extremely unlikely that users will resort to such measures in order to protect their personal information. Once this personally identifiable information has been submitted to a website the user has relinquished control over it. In order to conduct transactions over the web some level of trust must be established between the user and the company. The first and most important step in establishing rapport is providing sufficient notice of privacy practices to users.

B. Fair Information Principles

The FTC established the core tenets of privacy protection in a 1998 report by looking for common threads in data collection practices in the United States, Canada, and Europe.[120] The core tenets have become the closest thing to a best practices guide that the industry currently has. The primary principle, and the focus of the following sections, is that of notice. Individuals need to be made aware of what personal information is being collected, who is collecting it, how it is being used, and how it is shared with third parties. Once individuals have been informed of the data gathering practices, there should be made available a mechanism to provide consent. Most online companies use

---

Financial Cryptography (1997), p. 17, available at http://info.pittsburgh.intel-research.net/People/gibbons/papers/fc97.pdf.

[120] Federal Trade Commission, *Privacy Online: A Rreport to Congress* (June 1998), p. 7, available at http://www.ftc.gov/reports/privacy3/fairinfo.htm.

some combination of opt-in and opt-out schemes to provide consumers with the ability to specify how their personal information may be used. In addition to notice and consent, an individual should have access to stored information about him, and have some way of submitting corrections, as well as the means of filing a privacy complaint against a violating company. Companies should also provide a reasonable level of effort to secure collected personal information against intruders.

It is important to note that these principles are not independent of each other. Consent, access, and redress are only possible if individuals are provided proper notice. While self-regulation systems are often criticized on the basis of enforcement and redress, it is perhaps more important to first examine how well they communicate privacy practices to the end user.

C. Privacy Seals

Privacy seals are awarded to companies whose privacy notices meet certain prescribed minimum standards set by independent auditing agencies such as TRUSTe and BBBOnline. Sites that meet the standards are allowed to display an auditing agency privacy seal. Seal providers conduct random audits of member sites and also offer arbitration services to help settle privacy disputes. Participating companies pay seal providers based on a percentage of yearly revenue. Seal providers attempt to increase a consumer's trust level by vouching for a company's privacy practices.

TRUSTe's guidelines for drafting a privacy policy indicate that it should follow the Fair Information Principles for informing users of the company's data collection practices.[121] It is important to note that the privacy seal requirements do not enforce which information should be collected or how users should indicate consent. Sites are free to collect and use as much information as they want, so long as they explain what they are collecting in the privacy statement and provide users with opt-in or opt-out choices, the ability to access collected information, and information about how to submit complaints. The burden is on the user to read the statement and decide if the terms are acceptable. A recent survey indicates that only 3% of web surfers carefully read the

[121] TRUSTe, *Your Online Privacy Policy* (2004), p. 7, available at http://www.truste.org/pdf/WriteAGreatPrivacyPolicy.pdf.

privacy policies of the websites they visit.[122] 64% of users spend no time reading them or only occasionally glance at them.[123] Privacy seals do not function as well as notices because people are not reading them.

Despite industry's stated desire for self-regulation and urgings from Congress, privacy seal growth appears to be stagnant. A 2001 survey by the Progress and Freedom Foundation reported that only 12% of randomly sampled websites were displaying seals. At the time, TRUSTe claimed almost 2,000 members and BBBOnline had 760.[124] At the time of this writing, there are 1,458 participating TRUSTe websites[125] and 763 members for BBBOnline.[126]

One of the great benefits of the World Wide Web is the ability to connect any arbitrary set of pages together in a way that is both easy to author and easy to navigate for readers. Indeed, a Notre Dame study found that an average of only 19 clicks was needed to connect any two randomly selected websites.[127] The ease with which different pages on different sites can link together actually hinders the effectiveness of privacy seals. After clicking on a link, it is not always apparent to users which site they are viewing. Pages that open within frames compound this problem by not displaying the server name in the web browser's address bar. Most privacy statements contain disclaimers stating that the company is not responsible for the privacy practices of third party sites linked from its web pages. Even if users were to start reading privacy policies carefully, they may not realize when they have left the site where the statement applies and entered another site where a completely different policy may be in place. Clearly, a more automated approach for providing notice to users is needed.

---

[122] Harris Interactive, *Privacy Notices Research Final Results* (December 2001), p. 2, available at http://www.bbbonline.org/UnderstandingPrivacy/library/datasum.pdf.

[123] Ibid, p. 3

[124] William F. Adkinson, Jr. and Jeffrey Eisenach and Thomas Lenard,, *Privacy Online: A Report on the Information Practices and Policies of Commercial Web Sites* (March 2002), p. 25, available at http://www.pff.org/issues-pubs/books/020301privacyonlinereport.pdf.

[125] TRUSTe lists the total number of current members as of 15 September 2004, available at http://www.truste.com/about/fact_sheet.php.

[126] BBBOnline accessed on 30 November 2004, available at https://www.bbbonline.org/Business.

[127] Reka Albert and Hawoong Jeong and Albert-Laszlo Barabasi, *Diameter of the World-Wide Web*, Nature Magazine (May 1999), p. 130, available at http://www.nd.edu/~networks/Papers/401130A0.pdf.

D. P3P

The Platform for Privacy Preferences Project (P3P) is a standard for automatically communicating privacy policies to end-users. P3P is built on top of the existing HTTP standard and does not require the deployment of new web servers in order to implement it. Website operators can use the P3P standard to specify privacy practices in a machine-readable file that software tools, on the client side, can automatically download and interpret. The client software tools compare a website's P3P policy file to a predefined user profile and warn the user if the site does not meet his minimum privacy standards.

A P3P policy file is essentially a distillation of a website's privacy practices into a series of answers to multiple choice questions. The policy files are an attempt to create a standard way for websites to disclose information usage, how users indicate consents, how users can access personal information, and redress options. For example, the P3P standard dictates that policy files must disclose how each piece of personally identifiable information will be used. The description of each piece of collected data is annotated with one or more of 12 purposes. The data collection purposes include whether the information will be disclosed to third parties; whether the data will be kept for historical purposes; and whether if the data will be aggregated with other users and used for later analysis. Each purpose is further tagged as being opt-out, opt-in, or always collected.[128]

P3P requires support both from the website, to provide a policy file, and from the client to run user agents to parse the policy and compare it to a user profile. Microsoft's Internet Explorer 6 controls the placement of cookies using a stripped-down version of P3P known as "compact policy files."[129] The AT&T Privacy Bird is a more complete solution that is capable of parsing complete P3P policy files and integrating into Internet Explorer. Users can select a predefined low, medium, or high privacy profile, as well as tweak individual profile elements. If the user navigates to a site that conforms to his or her profile, a green bird appears in the browser toolbar. A red bird appears when opening

[128] W3C, *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification* (April 16, 2002), available at http://www.w3.org/TR/P3P/.
[129] Microsoft, *Press Pass - Information for Journalists*, available at http://www.microsoft.com/presspass/press/2001/mar01/PrivacyToolsIEfs.asp.

sites that conflict with a user's profile and a yellow bird is displayed if a site does not contain a P3P policy file at all.[130]

At first glance, P3P appears to solve the problems of providing notice that occur due to a user's failure to read privacy statements as well as not knowing when new policies are in effect. Unfortunately, like privacy seals, P3P suffers from a low industry adoption rate. Although the number of P3P compliant websites has been slowly increasing, a May 2004 Ernst & Young survey shows that only 24% of the top 500 websites have adopted P3P policy files.[131] Critics argue that creating policy files is a time consuming and difficult task and may not be feasible for smaller companies with fewer resources. Furthermore, it is problematic to try and shoehorn the expressiveness of a full privacy statement into small set of discrete options. Companies also fear the legal ramifications that may result from the loss of fidelity that occurs when translating a privacy statement into a P3P file.

An oft-repeated charge levied against P3P by privacy organizations such as the Electronic Privacy Information Center is that the standard does nothing to enforce a minimum set of privacy standards.[132] A website can create a policy file that states that personal information will be collected, aggregated with other information to create a profile, and then sold to third parties indiscriminately and still be deemed P3P-compliant. It is problematic however, to mandate a one-size-fits-all privacy standard that applies to all users. An individual may be comfortable providing information because it creates a more personalized browsing experience. That same individual may not want that information to be shared in a different context. For example, a user might enjoy seeing recommendations for similar CD's or books based on past purchases but not want browsing data to be captured when searching for material about an embarrassing medical condition. The burden of maintaining an individual's privacy standards should be placed on the P3P client tools run by the individual and not on the website itself. The responsibility of P3P client tools should be to provide adequate notice to a user so he can

---

[130] AT&T, *AT&T Privacy Bird Tour*, available at http://privacybird.com/tour/1_2_beta/tour.html.
[131] Ernst & Young, *P3P Dashboard Report: May 2004* (2004), p. 1, available at http://www.ey.com/global/download.nsf/US/P3P_Dashboard_-_May_2004/$file/E&YP3PDashboardMay.
[132] Electronic Privacy Information Center, *Pretty Poor Privacy: An Assessment of P3P and Internet Privacy* (June 2000), p. 5, available at http://www.epic.org/reports/prettypoorprivacy.html; Electronic Privacy

make an informed decision about his privacy. There are two main problems with trying to shift the responsibility of providing notice to client tools. First, there is the difficulty of informing users about the existence of P3P client tools in the first place. Although mainstream browsers such as Internet Explorer contain limited P3P implementations, more complete tools such as the AT&T Privacy Bird need to be downloaded and installed separately. The other, and perhaps more fundamental, problem is the fact that privacy often takes a backseat to functionality. In order to ensure that users are properly notified of privacy practices, P3P client tools need to default to more restrictive privacy settings and let users relax the constraints as needed. Unfortunately, many websites will not operate correctly without the placement of cookies and do not provide ways for users to turn off information collection. A survey of P3P-enabled websites found that 82% failed to meet the high privacy profile settings defined in the AT&T Privacy Bird tool.[133] P3P client tools often default to less restrictive settings in order to maintain a seamless browsing experience for the user. In the same way that users do not take the time to read privacy notices, users are also unwilling to tinker with the default settings of P3P client tools.

E. Improving Industry Adoption

Both seal programs and P3P suffer from a low industry adoption rate. Companies have little incentive to spend the time and money required to apply for a privacy seal or create a P3P policy file if consumers are currently willing to share personal information, they are in the dark about a company's data collection practices. Why should a company expend resources to provide better notice to users when it may create an aversion to sharing personal information at all?

A recent study demonstrated that users may in fact be more willing to share personal information if both the relevant portions of the privacy policy, along with the benefits of sharing information, are displayed in context.[134] In the study, a concise

---

Information Center, Ruchika Agrawal, *Why is P3P Not a PET?, W3C Workshop on the Future of P3P (2002), p. 7*, available at http://www.w3.org/2002/p3p-ws/pp/epic.pdf.

[133] Lorrie Cranor and Simon Byers and David Kormann, *An Analysis of P3P Deployment on Commercial, Government, and Children's Web Sites as of May 2003*, Federal Trade Commission Workshop on Technologies for Protecting Personal Information (2003), p. 11, available at http://www.research.att.com/projects/p3p/p3p-census-may03.pdf.

[134] Alfred Kobsa and Maximilian Teltzrow, *Cotenxtualized Communication of Privacy Practices and Personalization Benefits: Impacts on Users' Data Sharing and Purchase Behavior* to appear in Privacy

description of the relevant privacy practices along with the benefits of sharing was displayed next to the data entry fields in the web page itself. Providing users with better notice increases their ability to weigh the costs and benefits of information sharing. By incorporating contextualized privacy notices, companies may be able to increase their perceived commitment to privacy as well as obtain more data from better-informed users.

The results of this study suggest that privacy seals and P3P client tools may not be operating at the correct level of granularity. Both force users to make a decision up front whether to continue browsing without understanding how data sharing might be beneficial to them. A better solution would be to link user interface controls used in web pages such as text boxes and radio buttons with references to the section in the P3P policy file that describes what data the control is collecting. Armed with this additional information, P3P client tools would be able to display the relevant privacy implications to the user in context.

Increasing consumer awareness of data collection practices may drive companies to use higher default privacy settings for P3P client tools. It may be instructive to compare industry's treatment of privacy with its treatment of security. In the past, expanding a program's feature list would often override any security concerns. The proliferation of worms, viruses, and other vulnerabilities along with the ensuing negative media coverage changed the priorities of software makers. The recently released Service Pack 2 for Windows XP increased the default security settings of the operating system at the expense of maintaining compatibility with legacy applications.[135] If Microsoft were to add full P3P support to Internet Explorer, set the default privacy settings to a higher level, and let users re-adjust as needed, companies would be forced to adopt P3P in order to maintain compatibility given IE's dominant market share.

Despite industry protest to the contrary, the most expedient way to improve adoption might be to pass legislation requiring it. Lawmakers have a crucial role to play in the enforcement of the Fair Information Practices. It is of critical importance however, that any proposed legislation keeps the principle of notice in mind. Although self

---

Enhancing Technologies: Fourth International Workshop (2004), p. 1, available at http://www.ics.uci.edu/~kobsa/papers/2004-PET-kobsa.pdf.

[135] Joris Evers, *Windows XP SP2 Could Break Existing Applications* (March 4, 2004), available at http://www.infoworld.com/article/04/03/04/HNwindowsxpsp2_1.html.

regulatory measures may be a viable solution in the private sector, such measures will not solve privacy concerns as it relates to government. While government can protect individuals from privacy abuses by industry, there must also be a procedure in place to police the policemen. Even if private companies strictly adhere to their privacy policies, consumers will be loathe to share personal information if the government is allowed an escape clause to access sensitive data without restriction.

XI. Maintaining a Real Right To Privacy - Solutions

Differing solutions to the issue of privacy have been proposed. They can be summarized as follows:

1. technical solutions;
2. the EU data protection model of private sector regulation;
3. the American model of private sector self-regulation;
4. the American model of legislative patchwork; and, as discussed below,
5. a proposed Constitutional Privacy Amendment.

Technologies designed to meet the information requirements of business and government have effectively deprived private citizens of the power to control their personal information and profiling. Communication technologies, in addition to facilitating the gathering of detailed personal data, have enabled collectors and others to share data between themselves for unlimited purposes, without the knowledge or consent of ignorant online users. As discussed above, cookies, web beacons, browsers, search engines, and electronic commerce all play a role in the ongoing collection of data. Technical and regulatory initiatives like P3P, anonymizers, fair information principles, privacy seals, and the EU safe harbor principles play a corresponding role in an attempt to temper the collection of data.

The EU Data Protection Directive is flawed because it does not limit government data collection. Self-regulation is inadequate as applied to the U.S. government due to both a lack of enforcement and the absence of legal redress to harmed citizens. Arguably, self-regulation is successful in the private commercial sector because American businesses are fundamentally interested in making money, not just building databases on private citizens. Industry tends to favor self-regulation, arguing that it results in workable, market-based solutions. Since the U.S. private sector remains

comparatively free of regulation, it is motivated to make self-regulatory systems work. The private sector, however, is not armed with the unique powers to control police, the courts, and armies, like the government is.[136] Consequently, the commercial private sector does not provide the same level of concern that intrusion by the government does. Further patchwork legislation will probably prove to be no more effective than the present legislation.

People must own their private sensitive information. Current legislation dealing with varying pieces of the privacy puzzle suffers from the haphazard and chaotic way that it tries to deal with each situation as it arises. It is nothing more than a list of special causes that may become obsolete before it is even put into effect. Patchwork protection will no longer suffice. A generalized interest in information privacy calls for generalized protection. The effect of the Internet on our privacy is now greater than the Internet as a technology poses to information privacy, itself. As a result, the need for a legal regime that envisions more than simply protecting against particularized threats looms ever more necessary.[137] The patchwork approach clearly is inadequate for the larger task of protecting people's privacy as a whole. What is needed is a comprehensive and cohesive theory of privacy. We need clear guidelines on what is privacy. We need to grant the power to control private information to the citizen, himself. We need to focus on people, not technology.

XII. A Call For a Right To Privacy Amendment

Constitutional rights generate a foundational baseline commitment to rights that can be fleshed out by the courts and the legislature. Threats to privacy rights may very well be greater and different in the future, especially considering the present pace of changing technology. Legal protection schemes must therefore be adaptive.[138] Only a privacy right grounded in the Constitution can provide such flexibility. Such a commitment would avoid the many pitfalls of various alternative solutions discussed above. Amending the Constitution to add a universal right of privacy puts the power of

---

[136] Solveig Singleton, *Privacy and Human Rights: Comparing the U.S. and Europe* (Dec. 1, 1999), available at www.cato.org/pubs/wtpapers/991201paper.html.

[137] But see Michael Grossberg, *Some Queries About Privacy and Constitutional Rights*, 41 Case Western Reserve Law Review 857, at 860 (1991).

[138] Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, Berkeley Tech. Law Journal, issue 17:3, at 39-53 (2002).

controlling privacy back into the hands of the people. Statutes are too readily swept away by the changing winds of public opinion. Constitutional rights can only be invoked by the individual citizen, and are not tied to specific technologies. Such rights are "inalienable" and essentially guarantees against a fickle public.[139]

Due to the inadequacy of previously discussed solutions, the following proposed Amendment to the U.S. Constitution would best serve our collective interests in the right to privacy:

> The right of every person to a personal zone of privacy is recognized, and may not be infringed without a reasonable showing of a compelling state interest that may not be achieved in any less intrusive and reasonable manner. Such zone of privacy shall be held inviolate and shall include the right to control one's own body, property, all of one's personal information, protection from interception of one's thoughts and privileged communications by third parties by any means whatsoever, protection from unreasonable recording and tracking the activities and whereabouts of any citizen, and the right to be free from any form of government data collection, data analysis, and profiling.

Proposing a constitutional privacy Amendment may seem like an admission that such a right does not exist in the Ninth Amendment.[140] This argument goes back to the days of the Federalist Papers and dialogue between Thomas Jefferson, Alexander Hamilton, and James Madison. Protection of the un-enumerated rights in the Constitution rests solely on the Ninth Amendment. In the 215 years since the Constitution was ratified, the interpretation of Congress' enumerated powers has grown considerably. An enumerated powers argument in support of the right to privacy is not enough. Rights need to be enumerated to protect them from judicial and legislative infringement. The Ninth Amendment does not have the clout it was originally intended to have. Adoption of such a privacy Amendment would mean that it would apply to the states via the 14th Amendment, and to all persons acting as contractors or operating under color of law for the government. It would put the power to control privacy back with the citizen and form a powerful restraint against governmental abuse.

At present, the state constitutions of Alaska, Arizona, Colorado, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington already contain provisions

---

[139] Id.

[140] Chris lawrence, *Signifying Nothing, A Right to Privacy Amendment* (April 26, 2003), available at

for a constitutional right to privacy (or their Supreme Courts have recognized one).[141] Such states have cleared the path for the federal government to constitutionally protect our right to privacy.[142] Of course, while state constitutions only apply within that given state, such provisions apply to private parties as well as the state government. The federal Constitution does not apply similarly to private parties. It only applies to the state and federal governments.[143]

The Washington State Supreme Court may have succinctly described the situation best:

> The scope of constitutional protections should not diminish just because government conduct or technological developments diminish the degree of privacy that citizens actually expect.[144]

How does one successfully get the U.S. Constitution amended? Amending the Constitution is certainly not an easy task. There are essentially two ways spelled out in the Constitution itself, describing how it can be amended.[145] One method is for a proposed bill to pass both the Senate and the House of Representatives, by a two-thirds majority in each body. Once the bill has been passed by both halves of the federal legislature, it is sent to the 50 states for individual approval. A second, and never used, method is for a Constitutional Convention to be called by two-thirds of the legislatures of the various states, and for that Convention to propose one or more Amendments. Those Amendments would then be sent to the states for approval by three-quarters of the legislatures (or state conventions). In either instance, the Amendment must be approved by three-quarters of the total states. The Amendment as drafted may specify if the bill needs to be approved by the state legislatures or by special state conventions. Passage of the Amendment need only be accomplished at the state level by simple majority.

How often does this occur? There have been over 11,000 proposed Amendments. Twenty-seven Amendments have occurred since the inception of the Constitution. The

---

http://blog.lordsutch.com/?entryid=437.

[141] Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, Berkeley Tech. Law Journal, issue 17:3, at 39, 46-59 (2002).

[142] But, see obstructionist views in the fourth and sixth federal circuits. *Walls v. City of Petersburg*, 895 F2d 188 (4th Cir, 1990); *J.P. v. DeSanti*, 653 F2d 1080 (6th Cir, 1981)

[143] Shaun Helms, *Translating Privacy Values WithTtechnology*, 7 B.U. Journal of Science & Tech Law 288 (2001).

[144] *State v. Myrick*, 698 P2d 151 (Wash. 1994).

[145] See Article V of the U.S. Constitution

first ten were the original Bill of Rights. Nonetheless, the 24th, 25th, 26th, and 27th Amendments have been ratified during the past 40 years.

Changing the Constitution should never be taken lightly. Privacy rights, however, are not trivial in nature. The threat of living in a technological totalitarian state like the one described in George Orwell's "1984" is now very real. Freedom is a delicate balance of rights and duties, with powerful government machinery capable of being used for the benefit of the citizenry, or against the citizenry. We need a privacy Amendment to protect us from the most powerful government on earth and now is the time for concerned citizens to act.