Nova Law Review

Volume 23, *Issue* 2 1999 *Article* 2

Privacy in the Digital Age: Work in Progress

Jerry Berman* Deirdre Mulligan†

*

†

Privacy in the Digital Age: Work in Progress

Jerry Berman & Deirdre Mulligan*

TABLE OF CONTENTS

* Deirdre Mulligan is Staff Counsel at the Center for Democracy and Technology, a public interest organization dedicated to developing and implementing public policies designed to protect and enhance civil liberties and democratic values in the new digital media. Center for Democracy & Technology <http://www.edt.org>. This article was made possible through the generous support of the Deer Creek Foundation, and benefited from discussions with members of the Internet Privacy Working Group and various privacy and consumer advocates.

I. OVERVIEW

The Internet is at once a new communications medium and a new locus for social organization on a global basis. Because of its decentralized, open, and interactive nature, the Internet is the first electronic medium to allow every user to "publish" and engage in commerce. Users can reach and create communities of interest despite geographic, social, and political barriers. The Internet is an unprecedented mechanism for delivering government and social services, from education and healthcare to public information. As the World Wide Web grows to fully support voice, data, and video, it will become in many respects a virtual "face-to-face" social and political milieu.

However, it remains an open question whether the Internet's democratic potential will be achieved. The Internet exists within social, political, and technological contexts that can impede its democratic potential. Governments tout the Internet, but worry about its threat to their traditional authority. The private sector sees the economic potential of the Internet, but anti-competitive impulses are also part of the landscape. Users bring not only their social aspirations to the Internet, but also their potential for antisocial behavior. Adopting the frontier metaphor, we are now witnessing the struggle over governance of the Internet. After the revolution, what type of constitution do we want? Will it be pluralistic and democratic? Will it incorporate a bill of rights that protects individual liberty and equality?

Protection of privacy is one of the critical issues that must be resolved. Will the "Digital Age" be one in which individuals maintain, lose, or gain control over information about themselves? Will it be possible to preserve a protected sphere from unreasonable government and private sector intrusion? In the midst of this uncertainty, there are reasons for optimism. Individuals operating on the Internet can use new tools for protecting their privacy. From anonymous mailers and web browsers that allow individuals to interact anonymously, to encryption programs that protect e-mail messages as they pass through the network; individuals can harness the technology to promote their privacy. Equally important is the new found voice of individuals. Using e-mail, Web sites, listservers, and newsgroups, individuals on the Internet are able to quickly respond to perceived threats to privacy. Whether it be a proposal before the Federal Reserve Board requiring banks to "Know Your Customers,"[1] or the release of a product like

1. Notice of Proposed Rulemaking, 63 Fed. Reg. 67,563 (1998).

Intel's Pentium III, that will facilitate the tracking of individuals across the World Wide Web. Internet users have a forum for discussion, a simple method to find like-minded souls, and a platform from which to spread their message. This active vigilance is forcing the government and the private sector to reckon with a growing and vocal privacy constituency.[2]

But it is not just individuals' self-interest leading us toward increased privacy protection. Faced with numerous surveys documenting that the lack of privacy protections is a major barrier to consumer participation in electronic commerce, businesses are beginning to take privacy protection more seriously. Numerous efforts at self-regulation have emerged; both cooperative, such as TRUSTe,[3] the Better Business Bureau's Online Privacy Program,[4] and the Online Privacy Alliance;[5] and perhaps more importantly for the long-run, company specific. A growing number of companies, under public and regulatory scrutiny, have begun incorporating privacy into their management process and actually marketing their "privacy sensitivity" to the public. The collective efforts pose difficult questions about how to ensure the adoption and enforcement of rules in this global, decentralized medium.

Governments, are also struggling to identify their appropriate role in this new environment. To date, the United States policy appears to be largely based on the principle "first do no harm." The restraint shown thus far can be credited with providing the room for all affected parties to wrestle with the difficult issues presented by this new environment and move towards consensus. The principles to be abided by, and to some extent the enforcement schemes, are becoming more robust. Most importantly, the dialogue in recent months, evidenced by developments such as the recently passed Children's Online Privacy Protection Act ("COPPA")[6]—which was supported by children's advocates, privacy advocates, and companies—has taken an important turn. Less is heard about the means to achieve privacy protection—self-regulation versus legislation—and more focus is on the ends—privacy protections for individuals. These developments provide tangible evidence that common ground is within reach.

While expectations of privacy are under serious challenge, the self-interest of the various constituencies that make up the Internet—users, advocates, industry, and government—are all pushing toward the adoption of

---

2. Center for Democracy & Technology, *Privacy Not Price: Keeping People Off The Internet, CDT's Analysis of Recent Privacy Surveys* <http://www.cdt.org/privacy/survey/findings/surveyframe.html>.

3. *TRUSTe: Building a Web You Can Believe In* <http://www.etrust.org/>[hereinafter *TRUSTe*].

4. *BBB Online* <http://www.bbbonline.org/privacy/fr_bd_ix.html>.

5. *Online Privacy Alliance* <http://www.privacyalliance.org/>.

6. 15 U.S.C.A. § 6501 (1998).

technologies and rules that provide individuals with greater control over their information and their privacy.

II. WHAT MAKES THE INTERNET DIFFERENT?

If we are to design systems that protect privacy on the Internet—a globally, networked environment—we must understand the specific challenges to privacy posed by its functions and use. The Internet presents a series of new challenges for achieving public policy goals—be they protecting children from inappropriate material or protecting privacy.

A. *Increased Data Creation and Collection*

The Internet accelerates the trend toward increased information collection, which is already evident in our offline world. The data trail, known as transactional data, left behind as individuals use the Internet is a rich source of information about their habits of association, speech, and commerce. Transactional data, click stream data, or "mouse droppings," as it is alternatively called, can include the Internet protocol address ("IP address") of the individual's computer, the browser in use, the computer type, and what the individual did on previous visits to the Web site, or perhaps even other Web sites. This data, which may or may not be enough to identify a specific individual, is captured at various points in the network and available for reuse and disclosure. Some of the data generated is essential to the operation of the network, like the phone number that connects a calling party to the intended recipient, the IP address is necessary, for without it the network cannot function. However, other pieces of data may serve purposes beyond network operation. Along with information intentionally revealed through purchasing or registration activities, this transactional data can provide a "profile" of an individual's activities. When aggregated, these digital fingerprints reveal the blueprint of an individual's life. This increasingly detailed information is bought and sold as a commodity by a growing assortment of players.

B. *The Globalization of Information and Communications*

On the Internet, information and communications flow unimpeded across national borders. The Internet places the corner store, and a store three continents away, equally at the individual's fingertips. Just as the flow of personal information across national borders poses a risk to individual privacy, citizens' ability to transact with entities in other countries places individual privacy at risk in countries that lack privacy protections. National

laws may be insufficient, on their own, to provide citizens with privacy protections, across borders. Whether it is protecting citizens from fraud, limiting the availability of inappropriate content, or protecting privacy, governments are finding their traditional ability to make and effectively enforce policies challenged by the global communications medium.[7]

C. *Lack of Centralized Control Mechanisms*

While developing appropriate domestic policy may be sufficient in a paper-based world or a centralized and closed network, where nations can control the flow of information about citizens thereby protecting them from areas where protection is insufficient, information in a networked environment flows effortless from country to country, organization to organization, and policy regime to policy regime. Effective monitoring of the generation, collection, and flow of information on this vast scale may tax the resources of those currently responsible for data protection or other policies.

In addition to the difficulty of enforcing rules, governments around the globe are struggling with how to develop appropriate and effective rules. Efforts to use legal and regulatory instruments developed to address issues in other media—broadcast, telephone, print—may not be effective, and in cases like the United States' Communications Decency Act, may be found impermissible.[8] The need for global, decentralized solutions has prompted

---

7. The United States Congress' first effort to regulate speech on the Internet, the Communications Decency Act of 1996, Pub. L. No. 104–104, 110 Stat. 133 (codified as amended 47 U.S.C. 230 (1997)) [hereinafter "CDA"], was held to violate the First Amendment by the Supreme Court. Reno v. ACLU, 521 U.S. 844 (1997). Congress' second attempt, the Child Online Protection Act (Pub. L. No. 105-277, § 1401–06, 112 Stat. 2681 (1998)) (codified at 65 U.S.C.A. § 6501 (1998)) [hereinafter "CDA II"], is currently the subject of a legal challenge. On February 1, 1999, a federal district court issued a preliminary injunction prohibiting the government from enforcing CDA II until the court is able to issue a decision on its merits. ACLU v. Reno II, E.D. Pa. Case No. 98-5591, Preliminary Injunction Order (February 1, 1999). In contrast, the Clinton Administration's November report on Electronic Commerce advocates the voluntary use of filtering and blocking tools as the appropriate means of addressing concerns with children's access to inappropriate information on the internet. *See generally* U.S. Gov't Working Group, on Electronic Comm., First Annual Report (1998). The report also states that the Administration did not support CDA II. *See generally id.*

8. Concerns over children's access to inappropriate content were raised early on. Therefore, we have the most information about efforts to address this problem. We know that in the United States, applying standards developed for broadcast is unconstitutional. We have information about activities in other countries. Many have acknowledged the difficulty of controlling inappropriate content through regulation and are now looking toward decentralized user-controlled solutions to this problem. *See generally Global Internet Liberty Campaign Home Page* <http://www.gilc.org/>.

various international bodies including the European Union, the Organization for Cooperation and Development, and the United Nations to examine how to best advance their missions in this new environment.[9] As Dr. Malcolm Norris, Data Protection Commissioner for the Isle of Man, concluded in his paper, *Privacy and the Legal Aspects of the Information Superhighway*, "I believe the Internet will prove to be very difficult to govern in the way that Governments may wish."[10]

Together, the characteristics of the new medium pose challenges to our traditional, top-down methods of implementing policy and controlling behavior. Providing a seamless web of privacy protection to data as it flows through this international network will require us to harness the business community's interest in promoting commerce, the government's interest in fostering economic growth and protecting its citizens, and the self-interest of individuals in protecting themselves from the overreaching of the government and the private sectors. It requires us to use all of the tools at our disposal—international agreements, legislation, self-regulation, public education, and the technology itself. We must begin by reaching consensus on what we mean by protecting privacy, but we must keep the characteristics of the online environment sharply in focus. Concentrating in this manner is essential for the nature of the Internet and may alter the manner through which we achieve our goals.

III. WHAT DO WE MEAN BY PRIVACY? AND HOW IS IT BEING ERODED?

Privacy means many things to many people and different things in different contexts.[11] For the purpose of our discussion, we will examine

---

9. In October 1995, the European Union ("EU") adopted the Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 1995 J.O. (L28) 31. The Directive seeks to establish a common ground of privacy protection for personal data within the community and to ensure that the privacy of EU citizens was protected during "cross-border data flows,"—transfers of data to non-EU countries. *OECD guidelines on the Protection of Privacy and Transborder Flows of Personal Data* <http://www.oecd.org/dsti/sti/ii/secur/prod/PRIV_EN.HTM> [hereinafter *OECD Guidelines*]. Member States must comply with the Directive through the implementation of national provisions. *Id.* In February 1998, the OECD held a conference on Data Protection in International Networks. OECD Workshop on "Privacy Protection in a Global Networked Society" (February 1998) <http//www.oecd.org//dsti/sti/it/secur/prod/reg985final.pdf>. The Workshop provided an overview of various efforts to ensuring privacy protection. *See United Nations Human Rights Website*<http://www.unhchr.ch/html/menu3/b71.htm>.

10. Dr. Malcolm O. Norris, *Privacy and the Legal Aspects of the Information Superhighway* <http://www.odpr.org/restofit/Papers/Papers/Privacy_Internet.html>.

11. This discussion focuses primarily on information privacy. Information privacy

several core "privacy expectations"[12] that individuals have long held, and which should carry over to their interactions on the Internet that are under siege.

---

incorporates two components—at times distinct and at times inextricable—"the right to be let alone" first articulated by Justice Louis Brandeis over a century ago in his dissent in *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting), and the right to control information about oneself, even after divulging it to others, as discussed by Professor Alan F. Westin in *Privacy and Freedom*. *See generally* ALAN F. WESTIN, PRIVACY AND FREEDOM (Atheneum 1967). While there is no definitive case finding a constitutional right for information privacy, the Supreme Court acknowledged that such a privacy right exists in *Whalen v. Roe*, 429 U.S. 589, 605 (1977) (upholding a state statute that required doctors to disclose information on individuals taking certain highly addictive prescription drugs for inclusion on a state database). "The information . . . is made available only to a small number of public health officials with a legitimate interest in the information . . . . Broad dissemination by state officials of such information, however, would clearly implicate constitutionally protected privacy rights . . . ." *Id.* at 606. The lack of strong constitutional privacy protection has placed added emphasis on federal and state statutory protections. *See, e.g.*, The Privacy Act of 1974, 5 U.S.C. § 552a; Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g; The Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401; The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 (1995); The Communications Assistance and Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat 4279 (1994) (providing heightened protections for transactional data); The Cable Communications Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779 (1984) (codified as amended in scattered sections of 47 U.S.C.); The Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (1994); Consumer Credit Reporting Reform Act of 1996, 15 U.S.C. 1681-s2 (1997); Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994 , 15 U.S.C. §§ 6101–6108; Driver's Privacy Protection Act of 1994, 18 USC § 2721 (1994); Privacy of Customer Information (The Customer Proprietary Network Information Rules of the Telecommunications Reform Act of 1996), 47 U.S.C. § 222 (c), (d) (1996). While statutory privacy protections for personal information have been crafted on a sector by sector basis, many are based on a common set of principles set forth in the *CODE OF FAIR INFORMATION PRINCIPLES*, which was developed by the Department of Health Education and Welfare in 1973. *See generally* DEPARTMENT OF HEALTH EDUCATION & WELFARE, *CODE OF FAIR INFORMATION PRINCIPLES* (1973), in SECRETARY'S ADVISORY COMMITTEE REPORT ON AUTOMATED PERSONAL DATA SYSTEMS, *Records, Computers and the Rights of Citizens*, U.S. DEPT. OF HEALTH, EDUC. & WELFARE, July 1973.

12. The phrase "expectations of privacy" is used here with intent. Despite case law suggesting that the legal protections afforded to our expectations of privacy are limited by the technical and social possibilities for surveillance, the authors believe that, as a society, we do share some basic expectations of privacy. Privacy legislation enacted by Congress in response to some of the Court's decisions lends some credence to this notion.

The "reasonable expectation" test was articulated in the seminal privacy case, *United States v. Katz*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring), in which the Supreme Court ruled that the Fourth Amendment protects "people, not places" from unwarranted searches and seizures. *Id.* at 351. Thereby reversing *United States v. Olmstead*, 277 U.S. 438 (1928), which held that the Fourth Amendment covered only physical places, and thus the warrant requirement did not apply

A. *The Expectation of Anonymity*

Imagine walking through a mall where every store, unbeknownst to you, placed a sign on your back. The signs tell every other store you visit exactly where you have been, what you looked at, and what you purchased. Something very close to this is possible on the Internet.

When individuals surf the World Wide Web, they have a general expectation of anonymity, more so than in the physical world where an individual may be observed by others. If an individual has not actively disclosed information about herself, she believes that no one knows who she is or what she is doing. But the Internet generates an elaborate trail of data detailing every stop a person makes on the Web. This data trail may be captured by the individual's employer if she logged on at work, and is captured by the Web sites the individual visits.[13] Transactional data, click stream data, or "mouse-droppings," can provide a "profile" of an individual's online life.

---

to police wiretaps. *Id.* at 361 (Harlan, J., concurring). Although hailed as a landmark privacy decision, the *Katz* test has been applied in later cases to undermine privacy interests. In *Katz's* progeny, the Court has applied the "reasonable expectation" test as a relative standard informed by the technological and social realities of the day. As technology has advanced, and as societal demands for sensitive personal information have increased, the Court has increasingly circumscribed the "zones" one may justifiably consider private. *See* California v. Greenwood, 486 U.S. 35, 40–41 (1988) (quoting United States v. Reicherter, 647 F.2d 397, 399 (3d Cir. 1981) (holding that people have no reasonable expectation of privacy in garbage once it is removed from the home and placed on the curb for pick-up, because garbage is placed "'in an area particularly suited for public inspection and . . . for the express purpose of having strangers take it'")); California v. Ciraolo, 476 U.S. 207, 214–15 (1986) (holding that the use of a fixed-wing aircraft to observe marijuana on defendant's property from 1,000 feet did not violate his protected "zone of privacy" because the defendant's subjective expectation of privacy was not one "that society is prepared to honor . . . [i]n an age where private and commercial flight in the public airways is routine."). The Court's application of this standard has proved particularly troublesome in the information privacy context. The Court has continually held that individuals have no privacy interest in information divulged to the private sector, even though modern society leaves citizens no option but to disclose to others, e.g., disclosure as a condition of participation in society and technology accumulating transactional data. *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (holding that individuals have no privacy interest in the numbers dialed from their homes); United States v. Miller, 425 U.S. 435, 442–43 (1976) (holding that individuals have no reasonable expectation of privacy in personal financial records maintained by the bank). However, both *Smith* and *Miller* were later "overturned" by Congress through the enactment of statutes that created legally enforceable expectations of privacy. *See, e.g.*, 12 U.S.C. § 3401 (1994).

13. See The Center for Democracy and Technology's Snoop Demonstration at <http://snoop.cdt.org> for an example of the information that can be easily captured by sites on the World Wide Web.

Technologies such as "cookies,"[14] written directly onto your hard drive, enable Web sites to surreptitiously collect information about your online activities and store it for future use. Designed for the benign purpose of enabling Web sites to recognize a repeat visitor and respond accordingly, cookies were quickly adopted by Web sites to facilitate the tracking of specific individual's activities at Web sites for the purpose of customizing content and advertising. The surreptitious collection of information about individual's activities, across multiple Web sites enabled through some "cookie" implementations, gained the attention of Internet users, technicians, and policy makers.[15] Companies, such as Doubleclick, use this detailed transactional information to provide targeted online advertising. Others, such as Adfinity, combine these "mouse-droppings" or "click-stream data" with personal information collected from other sources into fully identifiable profiles of the individual's online and offline behavior.

The increased data collection enabled by the Internet and electronic commerce are part of a larger phenomena—the growing market in personal information. As one reporter stated:

> Let's face it: Companies are fascinated by me.
>
> Okay, maybe not me personally, but "me"—the consumer—collectively. I possess something nearly as valuable as spendable cash: information about myself. Before they can get to "me" to buy something, they need to know a lot about me: how old I am, how much I make, who I voted for, what I eat, wear, drive think or do.[16]

---

14. "Cookies" is a browser feature that assists Web site operators in tracking a user's activities. It was initially designed to address the "static state" problem of the World Wide Web, the fact that Web sites don't know whether a user is a first time or repeat visitor. *See* Joan E. Rigdon, *Internet Users Say They'd Rather Not Share Their 'Cookies,'* WALL ST. J., Feb. 14, 1996, at B6.

15. The initial response was the addition of a "cookie prompt" which alerts individuals that a Web site wishes to place a "cookie" on their browser. Peter Lewis, *Web Cookies: Trail of Crumbs*, SEATTLE TIMES: Search Results <http://archives.seattleti./display?storyID=55840 &query=cookie+AND+%22Ari+Schwartz%22>. Broader responses include the current attempt by members of the Internet Engineering Task Force ("IETF") to address privacy concerns with a rewrite of the "cookie" standard, and the availability of various technological tools that allow users to delete and/or disable "cookies." D. Kristol & L. Montulli, HTTP State Mangament Mechanism IETF Network Working Group, Request for Comments: 2109, D. Kristol Bell Laboratories, Lucent Technologies, L. Montulli Netscape Communications, February 1997 <http://www.ietf.org/rfc/rfc2109.txt>.

16. Paul Farhi, *ME INC.: GETTING THE GOODS ON CONSUMERS; Marketing Firms Want Basic Data About You and Me, But We're Wising Up to What Those Facts Are Worth*, WASH. POST, Feb. 14, 1999, at H01.

Evidence of the growing market for detailed "personal profiles" of individuals is rampant on the Internet. Be it personalized search engines and "portals," the pervasive use of "cookies" and other sticky bits of data that Web sites store on visitors' computers to aid the site in personalizing and targeting content and advertising, or the recent move by Intel to stamp each computer—and once the individual using the computer releases information, each individual—with a unique and traceable identity in cyberspace. The business communities rapacious appetite for information is all too apparent. Last August, some of the largest commercial sites on the World Wide Web announced that they would feed information about their customers' reading, shopping, and entertainment habits into a system developed by a Massachusetts company that was already tracking the moves of more than thirty million Internet users, recording where they go on the Internet and what they read, often without the users' knowledge.[17] In a sense, the system does what direct mail companies have done for years. But Internet based systems can be more precise, determining not only which magazines you subscribe to, but also which articles you read. More recently stories about "free" computers, valued at approximately $999, provided to individuals in exchange for detailed information about themselves and their families and permission to track their Internet usage, provide some indication of the value placed by a section of the business community on personal information and the lengths to which they will go to solicit it.[18]

While the private sector uses of personal information generated by use of the Internet have been scrutinized by the public and the press, the governments interest in and use of it has received less attention. But governments are interested in this data too. As the Federal Trade Commission revealed in its report to Congress on the Individual Reference Service Industry ("Look-up Services"), the government is a major customer of personal information about us.[19] While marketing information is not the fodder for "look-up services," it too is attractive to the government. A battle being waged today, over the "location" information available through many

17. Saul Hansell, *Big Web Sites to Track Steps of Their Users*, N.Y. TIMES ABSTRACT, Aug. 16, 1998, at 1, *available in* 1998 WL 5422846.

18. Karen Kaplan, *In Giveaway of 10,000 PCs, the Price is Users' Privacy Marketing: Recipients Must Agree to Let Pasadena Firm Monitor Where They Go on Internet and What They Buy*, L.A. TIMES, Feb. 8, 1999, at A1.

19. Individual Reference Services: FTC. *INDIVIDUAL REFERENCE SERVICES* 9 (Dec. 1997), *available in* 1997 WL 784156. The Individual Reference Services Industry is a sub-set of the information and industry which compiles information from the public and private sectors into information products that are used to locate, verify, and identify individuals, and provide dossiers of information about them. *See generally id.*

cellular networks, foreshadows the larger privacy considerations lurking in the vast data generated by individuals' use of the Internet.[20] In the course of processing calls, many wireless communications systems collect information about the cell site and location of the person making or receiving a call. Location information may be captured when the phone is merely on, even if it is not handling a call.[21] Both government and the private sector have their eye on this location information. While the government seeks to build added surveillance features into the network and ensure their access to the increasingly detailed data it captures, the private sector is considering how to use this new form of information. A company in Japan is experimenting with a World Wide Web site that allows anyone to locate a phone, and the person carrying it, by merely typing in the phone number.[22] As one reporter

---

20. In October of 1994, also commonly known as the "Digital Telephony" legislation, Congress enacted the Communications Assistance and Law Enforcement Act of 1994, providing heightened protections for transactional data. Pub. L. No. 103–414, 108 Stat 4279 (1994) (codified in scattered sections of 18 U.S.C. and 47 U.S.C.) [hereinafter "CALEA"]. The statute requires telecommunications carriers to ensure that their systems contain sufficient capability and capacity to permit law enforcement to conduct electronic surveillance. Although law enforcement officials must still obtain a search warrant in order to conduct a wiretap, the statute granted law enforcement new authority to influence the design of telecommunications networks. § 103(a), 108 Stat. at 4280.

Since its enactment, the Federal Bureau of Investigation ("FBI") has tried to use CALEA to require expanded surveillance features in the nation's telecommunications systems. Through statutory provisions which require public accountability and oversight over government design authority, telecommunications carrier liability, standards setting, and cost reimbursement, the Center for Democracy and Technology ("CDT") has attempted to curb the government's efforts to vastly increase surveillance capability. Telephone companies have yielded to some of the FBI's demands and have resisted others. In April 1998, acting upon a petition by CDT, the Federal Communications Commission ("FCC") launched an inquiry into whether the FBI's demands go farther than the law requires and infringe on privacy. Federal Communications Commission DA 98-762, *In the Matter of: Communications Assistance for Law Enforcement Act*, Docket No. 97-213 (April 20, 1998) (petition for Rulemaking under Sections 107 and 109 of the Communications Assistance for Law Enforcement Act, filed by the Center for Democracy and Technology). In September 1998, the FCC delayed implementation of CALEA by 20 months, until June 2000. In October 1998, the FCC tentatively approved many of the FBI's demands, including a proposal to turn cellular and other wireless phones into tracking devices. Action by the Commission, Memorandum Opinion and Order, FCC 98-223 (Sept. 10, 1998) (Chairman Kennard, Commissioners Ness, Powell and Tristani with Commissioner Furchtgott-Roth concurring and Commissioners Ness and Powell issuing a joint statement and Commissioner Furchtgott-Roth issuing a separate statement). At the same time, the FCC launched an inquiry into surveillance in pocket-switched networks. *Id.*

21. Albert Gidari, *Locating Criminals by the Book*, CELLULAR BUS., June 1996, at 70.

22. Edward W. Desmond, *The Scariest Phone System*, FORTUNE, Oct. 13, 1997, at 168.

put it: "Cellular telephones, long associated with untethered freedom, are becoming silent leashes."[23]

Now we head to the register. In the physical world, individuals can choose to purchase goods and services with a variety of payment mechanisms, the most common being cash, check, bank card, credit card, and a prepaid stored value mechanism, such as a travelers check or smart-card. Individuals can, and often do, pay by cash.[24] An individual's choice of payment mechanism impacts on her privacy. The amount of personal information generated and collected varies from theoretically none in a cash transaction to identity, item or service purchased, merchant, and date and time in a credit transaction. Similarly, the list of parties who have access to personal data can range from the individual and the merchant in a cash transaction, to the merchant, affiliated issuer, transaction processor, credit card company, and individual in a credit card transaction. In general, cash provides the most privacy protection during financial transactions in the offline world.[25] It is fungible, largely untraceable, and because its value is inherent and irrefutable, it requires no additional assurance of authenticity which often drives the collection of identity information.

In the online environment, the digital equivalent of cash has not yet achieved widespread use. Most online purchases are made with credit cards, which identify the individual and facilitate the collection of purchasing data. The lack of a cash equivalent in the online world, and its reduced use in the physical world, will seriously alter the privacy of individuals' financial dealings.[26]

For example, consider the differences between an auction/yard sale in the physical world and Ebay, the premiere auction/classified listing/yard sale on the World Wide Web. Attendees at a traditional auction while physically

23. Peter Wayner, *Technology that Tracks Cell Phones Draws Fire*, N.Y. TIMES ABSTRACTS, Feb. 23, 1998, at D3.

24. In many countries, offline consumer-initiated financial transactions are dominated by cash and checks. The reference is to the number of transactions not to the relative economic value they represent. Many of the transactions represented are likely to involve relatively modest sums. For example, newspaper purchases, meals, and phone calls to name a few. *See FRB: Federal Reserve Board Speech* from Mar. 7, 1997 <http://www.bog.frb.fed.us/boarddocs/speeches/19970307.htm> (remarks by Federal Reserve Board Chairman Alan Greenspan at the Conference on Privacy in the Information Age, Salt Lake City, UT, Mar. 1997).

25. However, even "ordinary cash itself, after all, is less than completely anonymous since it is usually exchanged in person, bears a unique serial number, carries fingerprints, and can easily be marked for identification." A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 471 (1996).

26. As financial transactions in the physical world continue to migrate to stored value cards, smart cards and chip-based systems, the need to build privacy protections into these payment systems becomes more urgent.

present do not reveal who they are prior to participation. At Ebay, prior to bidding individuals must provide a name, home address, phone number and e-mail address. The differences between the information collected to support a similar activity in these two environments to some degree reveals the increased emphasis placed on knowing the identity of the individual with whom you are interacting where the payment mechanism is less secure than what cash affords. The translation of cash, the most privacy protective of payment mechanisms, into an online equivalent, is a pressing privacy issue.[27] Without it we will quickly move from a world of cash-based anonymity to one of full identification and increased tracking of individuals' purchases.[28]

B. *The Expectation of Fairness and Control Over Personal Information*

When individuals provide information to a doctor, a merchant, or a bank, they expect that those professionals/companies will base the information collected on the service and use it for the sole purpose of providing the service requested. The doctor will use it to tend to their health, the merchant will use it to process the bill and ship the product, and the bank will use it to manage their account—end of story. Unfortunately, current practices, both offline and online, foil this expectation of privacy.

---

27. As Froomkin points out, a privacy-enhancing feature of digital cash transactions in general is that, unlike traditional financial transactions, they do not occur face-to-face. *Id.* at 471.

28. Law enforcement is eager to access the vast data available about individuals' financial transactions. Under a new set of proposed regulations, United States banks must monitor their customers and alert federal officials to "suspicious" behavior. The proposed regulations were filed with the Federal Register on December 7, 1998 by the Federal Deposit Insurance Corporation, the Federal Reserve, Department of the Treasury's Office of Comptroller of the Currency, and Office of Thrift Supervision. *See* Minimum Security Devices and Procedures and Bank Secrecy Act Compliance, 63 Fed. Reg. 67,529–67,536 (Dec. 7, 1998) (to be codified at 12 C.F.R. pt. 326). The regulations require banks to review every customer's "normal and expected transactions" and tip off the IRS and federal law enforcement agencies if the behavior is unusual. *Id.* Under the so-called "Know Your Customer" rules the Federal Reserve, the Office of Thrift Supervision, the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation have published identical requirements. *Id.* Today, if a bank detects any "suspicious activity," they must file a five-page report including your name, address, Social Security number, driver license or passport number, date of birth, and information about the transaction. *Id.* Under the new regulations they will also have to determine the "source of a customer's funds"—such as payroll deposits—and authorize federal agents to inspect "all information and documentation" of accounts upon request. *Id.* The information all goes into the Suspicious Activity Reporting System, a mammoth searchable database jointly administered by the IRS and FinCEN, around since April 1996. Over a dozen agencies including the FBI, IRS, Secret Service, bank regulators, and state law enforcement share access to this data. Declan McCullagh, *Banking With Big Brother, Wired News* <http://www.wired.com/news/print_version/politics/story/16749.html?wnpg=all>.

Whether it is medical information, or a record of a book purchased at the bookstore, information generated in the course of a business transaction is routinely used for a variety of other purposes without the individual's knowledge or consent. Some entities go so far as to declare the information individuals provide them as company "property."

There are multiple examples of companies using and disclosing personal information for purposes well beyond what the individual intended. For example, recent news stories have focused the public on misuses of personal health information by the private sector—particularly when it is digitized, stored and manipulated. Recently, the Washington Post reported that CVS drug stores and Giant Food were disclosing patient prescription records to a direct mail and pharmaceutical company.[29] The company was using the information to track customers who failed to refill prescriptions, and then sending them notices encouraging them to refill and to consider other treatments.[30] Due to public outrage and perhaps the concern expressed by senators crafting legislation on the issue of health privacy, CVS and Giant Food agreed to halt the marketing disclosures.[31] But the sale and disclosure of personal health information is big business. In a recent advertisement Patient Direct Metromail advertised that it had 7.6 million names of people suffering from allergies, 945,000 suffering from bladder-control problems, and 558,000 suffering from yeast infections.[32]

While many expect strong concern for privacy to surround sensitive information such as health and financial records, several recent incidents involving the sale and disclosure of what many perceive as less sensitive information indicate a rising of privacy concerns among the public.[33] In recent years, a number of corporations, as well as government entities, have learned the hard way that consumers are prepared to protest against services that appear to infringe on their privacy. In 1996, public criticism forced Lexis-Nexis to withdraw a service known as P-Trak, which granted easy online access to a database of millions of individuals' Social Security numbers. Also in 1996, Yahoo faced a public outcry over its People Search service. The service, jointly run with a marketing list vendor, would have

29. *See* Robert O'Harrow Jr., *Prescription Sales, Privacy Fears, CVS, Giant Shares Customer Records With Drug Marketing Firm*, WASH. POST, Feb. 15, 1998, at A1.

30. *Id.*

31. *See* Robert O'Harrow Jr, *CVS Also Cuts Ties To Marketing Service; Like Giant, Firm Cites Privacy on Prescriptions*, WASH. POST, Feb. 19, 1998, at E1.

32. Cheryl Clark, *Medical Privacy is Eroding, Physicians and Patients Declare*, SAN DIEGO UNION TRIB., Feb. 21, 1998, at B2.

33. *Internet Power Feeds Public Fear*, USA TODAY, Aug. 13, 1997, at B1. When news spread across the Internet about the availability of individuals' Social Security numbers through the Lexis-Nexis service P-track the public and policy makers were outraged. Pat Flynn, *Lexis-Nexis E-Mail Scare Proves Wrong*, SAN DIEGO UNIONTRIB., SEPT. 21, 1996, at C1.

allowed Net searchers to put an instant finger on 175 million people, all culled from commercial mailing lists. After hearing the complaints, Yahoo decided to delete 85 million records containing unlisted home addresses. During August of 1997, American Online ("AOL") announced plans to disclose its subscribers' telephone numbers to business partners for telemarketing.[34] AOL heard loud objections from subscribers and advocates opposed to this unilateral change in the "terms of service agreement" covering the use and disclosure of personal information.[35] In response, AOL decided not to follow through with its proposal.[36] At the beginning of the year, the Washington Post reported that several states had entered into agreements to sell state drivers' license photos to Image data. Under public scrutiny the deal seemed quite different,—state governors and legislatures quickly moved to block the contract. Florida Governor Jeb Bush terminated the contract saying: "I am personally not comfortable with the state mandating license photos for the purpose of identifying authorized drivers, and then selling those photos at a profit for a completely different purpose."

The technologies' surveillance capacity to collect, aggregate, analyze and distribute personal information coupled with current business practices have left individual privacy unprotected. While recent surveys[37] and public pressure have raised the privacy consciousness of companies, particularly those operating online,[38] individuals' information is frequently used and disclosed for purposes well beyond what the individual provided it for.

---

34. Rajiv Chandrasekaran, *AOL Will Share Users' Numbers for Telemarketing*, WASH. POST, July 24, 1997, at E1; Rebecca Quick, *Soon AOL Users Will Get Junk Calls, Not Just Busy Signals and E-mail Ads.*, WALL ST. J., July 24, 1997, at B6. Its important to note that while AOL has been taken to task for failures to protect subscribers privacy, the AOL privacy policy has been recognized by many advocates as one of the best in the industry. *See Department of Commerce Workshop on Online Privacy*, June 1998 <http://www.doc.gov/>.

35. *See* Letter from the Center for Democracy and Technology, Electronic Frontier Foundation, EFF-Austin, National Consumers League, Privacy Rights Clearinghouse, and Voters Telecommunications Watch to Steve Case, President, AOL (on file with the author).

36. Rajiv Chandrasekaran, *AOL Cancels Plan for Telemarketing; Disclosure of Members' Numbers Protested*, WASH. POST, July 25, 1997, at G1.

37. For an overview of recent surveys of consumer concerns with privacy see, *The Center for Democracy and Technology*, <http://www.cdt.org/privacy/surveys/findings/introbody.html>.

38. The "Online Industry" has been active on the privacy front by creating self-regulatory principles, funding and developing mechanisms to provide accountability and service consumer complaints, and developing seals to identify Web sites that abide by industry-developed privacy guidelines. *See Online Privacy Alliance*, *supra* note 5; *BBB OnLine*, *supra* note 4; *TRUSTe supra* note 3.

C. *The Expectation of Confidentiality*

When individuals send an e-mail message, they expect that it will be read only by the intended recipient. Unfortunately, this expectation too is in danger. For starters, if an individual is using an office computer, it is possible, and legal, for her boss to monitor her messages. If she is using her home computer, her privacy is still not fully assured.

While United States law provides e-mail the same legal protection as a first class letter, the technology leaves unencrypted e-mail as vulnerable as a postcard. Compared to a letter, an e-mail message travels in a relatively unpredictable and unregulated environment. As it travels through the network, e-mail is handled by many independent entities: in comparison, a letter is handled only by the United States Postal Service. To further complicate matters, the e-mail message may be routed, depending upon traffic patterns, overseas and back, even if it is a purely domestic communication. While the message may effortlessly flow from nation to nation, the statutory privacy protections stop at the border. In addition, unlike the phone or postal systems, the Internet does not have central points of control. While the decentralized nature of the Internet allows it to cope with problems and failures in any given computer network, by simply routing in another direction, it also provides ample opportunities for those seeking to capture confidential communications.[39] The rogue action or policy of a single computer network can compromise the confidentiality of information.

But e-mail is just one example, today our diaries, our medical records, our communications, and confidential documents are more likely to be out in the network than under our bed. This has drastic consequences for our privacy—as information moves further out onto the network our existing statutory framework provides less and less protection.

It's useful to look at the weak state of privacy protections for other personal papers and records. Individuals traditionally kept their diaries under their mattress, in the bottom drawer of their dresser, or at their writing table. Situated within the four walls of the home, these private papers are protected by the Fourth Amendment. With the advent of home computers, individual diaries moved to the desktop and the hard drive. Writers, poets, and average citizens quickly took advantage of computers to manage and

39. Attempts to regulate the availability of encryption on the Internet highlight the frustrations that regulators may experience. As many scholars and advocates have pointed out, national attempts to restrict the availability of encryption are likely to be ineffective. For if even one jurisdiction or one network in one jurisdiction fails to restrict it, individuals worldwide will be able to access it over the Internet and use it.

transcribe their important records and thoughts. Similarly, pictures moved from the photo album to the CD-ROM.

Today, network computing allows individuals to rent space outside their home to store personal files and personal World Wide Web pages. The information has remained the same. A diary is a diary is a diary. But storing those personal thoughts and reflections on a remote server eliminates many of the privacy protections they were afforded when they were under the bed or on the hard drive. Rather than the Fourth Amendment protections—including a warrant based on probable cause, judicial oversight, and notice—the individual's recorded thoughts may be obtained from the service provider through a mere court order with no notice to the individual at all.

The weak state of privacy protection is evident in the business setting too. Let's look at medical records. Hospitals, their affiliated clinics, and physicians are using intranets to enable the sharing of patient, clinical, financial, and administrative data. Built on Internet technologies and protocols, the private networks link the hospital's information system, to pharmacy and laboratory systems, transcription systems, doctor and clinic offices and others. The United States government is contemplating the development of a federal government-wide computer-based patient record system.[40] According to news reports, the Internet and World Wide Web-based interfaces are under consideration.[41] The private sector is moving to integrate network computing into a sensitive area of our lives, the doctor's office.[42]

As computing comes to medicine, the detailed records of individuals' health continue to move not just out of our homes, but out of our doctor's offices. While the use of network technology promises to bring information to the fingertips of medical providers when they need it most, and greatly ease billing, prescription refills, and insurance preauthorizations, it raises privacy concerns.

In the absence of comprehensive federal legislation to protect patient privacy, the legal protections afforded medical records may vary greatly depending upon how the network is structured, where data is stored, and how long it is kept. If records are housed on the computer of an individual

---

40. *Why the Government Wants a Computerized Patient Record*, Health Data Network News, Vol. 7, No. 6, Mar. 20, 1998, at 1.

41. *Id.* at 8.

42. *See generally Six Boston Hospitals Turn To the Internet as a Clinical Network Tool*, Health Data Network News, Vol. 6, No. 6, June 20, 1997, at 1; *More Clearinghouses Conclude the Internet Makes Economic Sense*, Health Data Network News, Vol. 6, No. 6, June 20, 1997, at 1; *Hospital Banks on Web Technology for Integration*, Health Data Network News, Vol. 6, No. 16, Nov. 20, 1997, at 3.

doctor then access to that data will be governed by the Fourth Amendment.[43] Law enforcement would be required to serve the doctor with a warrant or subpoena and the doctor would receive notice and have the chance to halt an inappropriate search. Under federal law, the patient however, would receive no notice and have no opportunity to contest the production of the records. When information is in transit between a doctor and a hospital through a network, law enforcement's access is governed by the warrant requirements of The Electronic Communications Privacy Act of 1986 ("ECPA"); and, neither doctor nor patient receive prior or contemporaneous notice. If the records are stored on a server leased from a service provider, the protections are unclear. They may be accessible by mere subpoena. If they are covered by the "remote computing" provisions of ECPA this would severely undermine privacy in the digital age.[44]

The confidentiality of our sensitive information is challenged by a legal framework that hinges protections on who maintains the information, how the network is structured, where data is stored, and how long it is kept. As our wallets become "e-wallets" housed somewhere out on the Internet rather than in our back-pockets, and as our public institutions, businesses, and even cultural institutions find homes online, the confidentiality of our communications, papers, and information is at risk of compromise.

IV. WHERE DO WE GO FROM HERE?

It is clear that our existing legal framework did not envision the pervasive role information technology would play in our daily lives. Nor did it envision a world where the private sector would collect and use information at the level it does today. Our legal framework for protecting individual privacy in electronic communications while built upon constitutional principles and statutory protections, reflects the technical and social "givens" of specific moments in history. From a belief that the government's collection and use of information about individuals' activities and communications was the only threat to individual privacy and that a solid wall separated the data held by the private and public sector; to the notion that the Internet would be used primarily for a narrow slice of activities and that private and public spaces were easily demarcated, these

43. The recordkeeper would have Fourth Amendment protections. Whether the patient's privacy is protected at all would largely depend upon state law, which is scattered and inconsistent. Until a federal law protecting individual's privacy in health information is crafted to protect data regardless of where it is stored or whose control it is under, privacy is in danger.

44. 18 U.S.C. § 2703(b) (1994).

vestiges of a pre-Internet, pre-networked world, stress our existing privacy framework.

Crafting proper privacy protections in the electronic realm has always been a complex endeavor. It requires a keen awareness of not only changes in technology, but also changes in how the technology is used by citizens, and how those changes are pushing at the edges of existing laws. From time to time these changes require us to reexamine our fabric of privacy protections. The issues raised in this article indicate that it is time for such a review.

The Internet has changed the quantity and quality of data available about individuals' lives, but unfortunately our business practices, norms, and laws have not progressed to ensure individuals' privacy. At the outset, there are six areas where we must step up our activities to strengthen privacy protections. Clear proposals can be attached to some, while at this time others require further consideration.

A. *Maintain a Consistent Level of Privacy Protection for Communications and Information Regardless of Where They are Stored*

Increasingly, our most important records are not "papers" in our "houses" but "bytes" stored electronically at distant "virtual" locations for indefinite periods of time and held by third parties. As discussed in Part I, the Internet, and digital technology generally, accelerate the collection of information about individuals' actions and communications. Our communications, rather than disappearing, are captured and stored as well on servers controlled by third parties. With the rise of networking and the reduction of physical boundaries for privacy, we must ensure that privacy protections apply regardless of where information is stored.

Under our existing law, there are now essentially four legal regimes for access to electronic data: 1) the traditional Fourth Amendment[45] standard for records stored on an individual's hard drive or floppy disks; 2) the Title III-Electronic Communications Privacy Act[46] standard for records in transmission; 3) the standard for business records held by third parties, available on a mere subpoena to the third party with no notice to the individual subject of the record;[47] and 4) for records stored on a remote server such as the research paper, or the diary, of a student stored on a university server, or the records, including the personal correspondence, of

45. U.S. CONST. amend. IV.
46. 18 U.S.C. §§ 2570–2711 (1994).
47. Fed. R. Civ. P. 45(b)(1).

an employee stored on the server of the employer, the scope of which is probably unclear.

As the third and fourth categories of records expand because the wealth of transactional data collected in the private sector grows and people find it more convenient to store records remotely, the legal ambiguity and lack of strong protection grows more significant and poses grave threats to privacy in the digital environment. Independent Counsel Starr's investigation into books purchased by Monica Lewinsky highlights the potential sensitivity of records routinely collected by businesses and the intersection of privacy and First Amendment concerns.[48] During his investigation into President Clinton's relationship with White House intern Monica Lewinsky, Starr sought information confirming the purchase of a specific book by Miss Lewinsky. Starr served a subpoena upon Kramer Books, a local DC bookstore, demanding the production of records reflecting purchasing activities.[49] While the book store valiantly objected to the subpoena on First Amendment and privacy grounds, and Starr eventually obtained Miss Lewinsky's records through other channels, this incident raised concern among the book-buying public.[50] To search Miss Lewinsky's residence for information about her reading habits Starr would have needed a warrant, but in the hands of the bookstore the records were available under a less stringent standard.

Sometimes the equation is flipped—the government has collected the data and the private sector seeks access to it. During the law suit brought by several states, including Massachusetts, against the tobacco industry for repayment of state health care costs for smoking related illnesses, lawyers for the tobacco industry sought access to a Massachusetts database containing records on every hospital visit by every person in the entire state population.[51] While the State's purpose for collecting the data was to compare what it paid for health care to private insurers, it failed to enact privacy protections to limit access to the database.[52] Because the State's argument for repayment was premised on its ability to prove damage to state residents from tobacco products, the tobacco companies wanted to see the data supporting it.[53] Massachusetts acted responsibly, hiring a team of

48. DAVID STOUT, *Lewinsky's Bookstore Purchases Are Now Subject of a Subpoena*, N. Y. TIMES, Mar. 25, 1998, at A1.

49. DOREEN CARVAJAL, *Testing a President: The Investigation; Book Industry Vows to Fight 2 Subpoenas Issued Kenneth W. Starr*, N.Y. TIMES, Apr. 2, 1998, at A1.

50. STEPHEN LABATON, *Lewinsky's Lawyers to Turn Over Records of Book Purchases*, N. Y. TIMES, June 22, 1998, at A1.

51. John Schwartz, *Private Data, Public Worries*, WASH. POST, June 8, 1998, at F24.

52. *Id.*

53. *Id.*

cryptographers to ensure that the data released wouldn't identify individuals, however the fact remains that the data was not protected by law.[54]

Even our communications are vulnerable under today's law. Under the existing legal framework, the same e-mail message would be afforded different privacy protections depending on whether it was sought: while on the individual's computer; in transmission; unread in storage for less than 180 days; or, read but left on the service provider's server. The differences in protection afforded e-mail depending on whether it is captured in transmission, accessed in storage while unread, or accessed in storage after it has been read seem unwarranted, for the communication and individuals' expectations of privacy remain the same. In an era where e-mail is more commonly accessed as a stored record than through an interception, the concepts developed for governmental access to business records in the relatively static, paper-based environment are an ill-fit and provide weak protections for individual privacy. It is time to provide a framework that reflects individuals' expectations.

B. *Raise the Legal Protections Afforded to Transactional Data When it is Collected*

Where information is needed, we must ensure that it is protected from misuse and unfettered government access. Congress acted by legislation to establish a right of privacy in bank records in the wake of a Supreme Court decision finding they were without constitutional protection.[55] Institutions all across the economy are quickly becoming store houses of information about individuals' marketplace behaviors,—unlike records held by banks, these new databases are unprotected. The possibilities of computer analysis have given value to tidbits previously considered meaningless: the little digital footprints individuals leave showing who they called, where they used their credit cards, what websites they visited, what products they purchased, and when they entered the "intelligent" highway using the automatic toll booth. While a certain website or product registration card may only ask for a few minor pieces of personal information, together they constitute a fairly complete profile of one's associations, habits, health condition and personal interests, combining credit card transactions with magazine subscriptions, telephone numbers, real estate records, car registrations and fishing licenses.[56] The digital deposits of these transactional

54. *Id.*

55. United States v. Miller, 425 U.S. 435 (1976).

56. ROBERT O'HARROW, JR., *Data Firms Getting Too Personal?*, Wash. Post, Mar. 8, 1998, at A1.

details are so deep that the practice of exploiting their commercial value is called "data-mining," evoking the intensive, subterranean, and highly lucrative labors of an earlier age.

It's time to ensure that the records of our reading habits, our online browsing, and all the details of our lives left behind, online and in electronic commerce, are not treated as mere "business records" available, without our knowledge or permission, at the government's request. For even the most mundane of records can harbor risks to privacy. A December Washington Post article revealed that Drug Enforcement Administration ("DEA") officials were reviewing records of grocery store purchasing data collected to support "frequent shopper" or loyalty programs.[57] What would DEA officials possibly hope to uncover? According to the Post, they were seeking to identify purchasers of large numbers of small plastic bags and baking powder — common grocery supplies used by drug dealers to dilute and package cocaine and other drugs.[58] As businesses intensify their data collection efforts we must take steps to strengthen the privacy protections afforded this data.

Congress took the first small step towards recognizing the changing nature of transactional data in the networked environment with amendments to the Electronic Communications Privacy Act[59] enacted as part of the Communications Assistance for Law Enforcement Act of 1994 ("CALEA").[60] The 1994 amendments recognized that transactional data was emerging as a hybrid form of data, somewhere between addressing information and content, and was becoming increasingly revealing of personal patterns of association. For example, addressing information was no longer just a number and name, but contained the subject under discussion and information about the individual's location. Therefore, Congress raised the legal bar for government access to transactional data by eliminating subpoena access and requiring a court order, albeit one issued on a lower relevance standard.[61] This Congress passed legislation to foster online interactions between citizens and the government by facilitating the

57. ROBERT O'HARROW, JR., *Bargains at a Price Shoppers' Privacy, Cards Let Supermarkets Collect Data,* WASH. POST, Dec. 31, 1998, at A1. *See also* ROBERT O'HARROW, JR. *Behind the Instant Coupons, A Data Crunching Powerhouse*, WASH. POST, Dec. 31, 1998, at A20.

58. ROBERT O'HARROW, JR., *Bargains at a Price Shoppers' Privacy, Cards Let Supermarkets Collect Data,* WASH. POST, Dec. 31, 1998, at A1.

59. 18 U.S.C. §§ 2510–2711 (1994).

60. Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. § 1001 and scattered sections of 18 U.S.C. and 47 U.S.C.).

61. 18 U.S.C. § 2703(b)(2)(A)–(B), (c)(1)(B), (d) (1994).

government's acceptance of digital certificates.[62] The legislation includes forward looking privacy protections for the transactional data generated by citizens' use of digital certificates.[63] On a case by case basis, the courts are addressing the privacy issues raised by this revealing data. However, as electronic commerce becomes pervasive, transactional data will continue to proliferate. A piecemeal approach may not provide the privacy protections that this potentially sensitive information deserves.

C. *Encourage Technologies that Limit the Collection of Personally Identifiable Data*

Law is only one tool for protecting privacy. In this global, decentralized medium, we must promote applications of technology that limit the collection of transactional information that can be tied to individuals.[64] Some tools developed to protect privacy by limiting the disclosure, or cloaking it, of information likely to reveal identity, or decoupling this identity information from the individual's actions and communications, exploit the decentralized and open nature of the Internet.[65] For example, Crowds provides anonymity to individuals surfing the Web by mingling their requests for access to Web sites with those of others.[66] By routing Web site access requests in a series of unpredictable paths, the identity of the requester is hidden. Similarly, Onion Routing uses the decentralized nature of the Internet coupled with public key encryption to provide privacy protections for Internet communications.[67] Communications

---

62. The Government Paperwork Elimination Act, Pub. L. No. 105–277, §§ 1701–1710, 112 Stat. 2681, 2681–749 (1998) (codified at 44 U.S.C.A. § 101 (1998)).

63. § 1708, 112 Stat. at 2681–750.

64. For a thoughtful discussion of the privacy protection possible through technologies that limit data collection, see THE NETHERLANDS AND INFORMATION AND PRIVACY COMMISSIONER, I, II *Privacy-Enhancement Technologies: The Path to Anonymity* (Ontario, Canada Aug. 1995) [herinafter NETHERLANDS]. In his paper, "Privacy-Enhancing Technologies: Typology, Critique, Vision," Herbert Burkert suggests that Privacy-Enhancing Technologies ("PETs") can be differentiated into four categories: subject-oriented; object-oriented; action-oriented; and, system-oriented. Burkert's approach provides a heuristic method useful for thinking broadly about the role of PETs. Herbert Burkert, *Privacy-Enhancing Technologies: Typology, Critique, Vision*, in TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE, 125–142 (Philip E. Agre & Marc Rotenberg, eds. MIT Press 1997).

65. For a review of several privacy-enhancing technologies see, volume 42, no. 2, Feb. 1999 of the Communications of the ACM on Internet Privacy, guest editor Lorrie Faith Cranor. February 1999.

66. *Crowds Home Page* < http://www.research.att.com/projects.crowds/>.

67. David Godschlag et. al., *Onion Routing: Publications Onion Routing for Anonymous and Private Internet Connecting* <http://www.onionrouter.net/publications/html>.

are passed through a series of routers before reaching the recipient. Resembling an onion, the message is encircled in a series of layers. Each router is able to peel one layer of the onion enabling it to learn the next stop in the messages path. Passing messages in this fashion protects an individual's identity by obfuscating the originator and recipient of the message from points in the network. These technical advances, if adopted by users, can provide protections for privacy.

Of particular importance are payment mechanisms that preserve anonymity. By using cash, individuals can engage in many daily transactions without revealing their identity. Depending on the design choices we make, the online environment could wipe out the expectation of privacy that the physical world's cash purchase provides or the technology of electronic payments could preserve privacy. Similarly, digital certificates, if guided by privacy concerns, could be designed to limit the instances in which identity is used as a broad substitute for specific traits or abilities.

A number of companies have attempted to craft cash-like payment mechanisms.[68] Digicash is a frequently mentioned payment mechanism that provides cash-like anonymity to individual users.[69] Digicash relies on blind digital signatures, a cryptographic technique, to prevent the bank, or other money issuer, and merchant from linking the individual's identity to specific transactions.[70] Blind signatures provide the merchant with the ability to determine the value and establish the authenticity of the payment while shielding the individual's identity. The bank, while privy to information about the user's identity, and able to deduct the appropriate sum from the individual's account, is incapable of tying the particulars of a transaction to the individual.[71]

---

68. Catherine Lee Wilson, *Banking on the Net: Extending Bank Regulation to Electronic Money and Beyond*, 30 CREIGHTON L. REV. 671 (1997).

69. *Digi-Cash Welcome* <http://www.Digi-Cash.com./digicash/index.html>. However, unlike cash, Digi-Cash in its current applications does not provide anonymity to the recipient. Generally, other available digital cash systems use digital signatures but do not provide for anonymity.

70. *Ecash-An Introduction to ecash* <http://www.digicash.com/ecash/intro/index.html>. Digi-Cash couples its blind digital signature technology with online clearing of transactions. *Id.* Online clearing of transactions means that prior to accepting a payment the recipient is able to check to ensure the obligation will be met. *Id.* This is similar to the online check used in credit card authorization. *Id.*

71. *Id.* The decoupling of accounting and identity are facilitated by front-end debiting. The user produces a digital document containing both her identity and a pseudonym. She sends it to her bank with only the identity readable. The bank verifies the document, deducts the appropriate amount from her account, and sends it back to the user as a document of fixed value with a stamp indicating its authenticity. The user then gives the digital document to a merchant obscuring her identity and revealing her pseudonym. The merchant can read the value and the

The ability to engage in cash-like transactions in the online environment is important to the protection of privacy. The enhanced data generation and collection that occurs during the process of browsing a virtual store front, a merchant's World Wide Web site, increases the privacy concerns associated with the revelation of identity during the payment process. The capacity to connect information far in excess of the specifics of a given financial transaction to the individual's identity increases the risks to individual privacy relative to the concerns in the offline world.

Digital cash technology can vastly reduce the need for the collection and revelation of identity information. By providing alternative methods of authenticating value, the online environment can afford cash-like anonymity while providing some of the protections against theft associated with traditionally data intensive payment mechanisms. For example, Digicash's reliance on blind digital signatures may limit the risk of theft by providing for non-identity dependent methods of verifying the transaction at the point that value is removed from the individual's account.

The development of electronic payment mechanisms that protect privacy hinges on the use of strong cryptography and the creation of a robust public key infrastructure to support its use.[72] By designing payment mechanisms to limit the collection of personally identifiable information by banks, clearinghouses, and merchants, it is possible to preserve the privacy which individuals currently enjoy during cash transactions and perhaps move the developers of other payment mechanisms to enhance privacy protection. The private sector and the government should foster the development of payment mechanisms and other technologies that foster anonymity and privacy.

D. *Establish Rules and Implement Technologies That Give Individuals Control Over Personal Information During Commercial Interactions*

We must adopt enforceable standards, both self-regulatory and regulatory, to ensure that information provided for one purpose is not used or redisclosed for other purposes. At the same time, we must recognize that in this freewheeling, open marketplace, there will be limits to the effectiveness of regulation and self-regulation. Therefore, we must look to technological tools that will empower individuals to control their personal information.

---

stamp on the document indicating its authenticity. When presented to the bank the merchant's account will be credited. *See* NETHERLANDS, *supra* note 64, at 40–42.

72. Law enforcement desires to monitor financial transactions and the interest of merchants and others involved in commerce in exploiting data about individuals for marketing purposes may be a barrier to the market adoption of privacy-protective electronic payment mechanisms.

The Federal Trade Commission and the Department of Commerce are engaged in initiatives designed to promote "fair information practice principles" in the online environment. The business community is also engaged in efforts to protect privacy through self-regulatory guidelines and enforcement mechanisms. All such efforts should focus on the Code of Fair Information Practices ("CFIP") developed by the Department of Health, Education and Welfare ("HEW") in 1973[73] and the Guidelines for the Protection of Privacy and Transborder Flows of Personal Data, adopted by the Council of the Organization for Economic Cooperation and Development in 1980.[74] Coupled with the World Wide Web Consortium's Platform for

---

73. Secretary's Advisory Comm. on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens,* U.S. Dept. of Health, Education and Welfare, July 1973.

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

Id.

74. 1. Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data quality: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose specification: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use limitation: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the "purpose specification" except: (a) with the consent of the data subject; or (b) by the authority of law.

Privacy Preferences ("P3P")[75], rules based on the FIP will provide a framework that protects privacy by limiting data collection to that which is necessary for transactions and ensuring that individuals are the arbiters of their personal information. The challenge of implementing privacy practices, such as notice and consent, on the Internet is ensuring that they are implemented in a fashion that builds upon the medium's real-time and interactive nature and uses it to foster consumer privacy.

While the path to this policy is currently quite contested, there is some indication of a growing willingness to collaborate in order to develop privacy protections. Debate over the capacity of self-regulation and market forces to adequately address privacy concerns is common in the privacy and consumer protection arenas, and will continue to rage. Advocates often take the position that self-regulation is inadequate due to both a lack of enforcement and the absence of legal redress to harmed individuals. Industry tends to strongly favor self-regulation, stating that it results in workable, market-based solutions while placing minimal burdens on affected companies. These positions, while in tension, have both accurately

---

5. Security safeguards: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. Openness: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual participation: An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him:

- within a reasonable time;
- at a charge, if any, that is not excessive;
- in a reasonable manner; and,
- in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and, (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified completed or amended.

8. Accountability: A data controller should be accountable for complying with measures which give effect to the principles stated above.

OECD Guidelines, supra note 9.

75. For an overview, *see* Joseph Reagle & Lorrie Faith Cranor, *The Platform for Privacy Preferences*, Comm., at 48–55.

described the self-regulatory process. A close look at the enactment of federal privacy legislation over the years reveals that the battle itself, with all its sound and fury, is the path to legislation.

Historically, for privacy legislation to garner the support of at least a section of the industry, which is generally critical to successful legislative efforts, it must build upon the work of some industry members—typically binding bad actors to the rules being followed by industry leaders—or, be critically tied to the viability of a business service or product as with the Video Privacy Protection Act and the Electronic Communications Privacy Act.[76]

---

76. The Electronic Communications Privacy Act of 1986 (ECPA), which updated the 1968 Wiretap Act, was the result of a collaborative public interest/private sector effort. 18 U.S.C. §§ 2510–2711 (1994). Industry feared that without legal protection against eavesdropping and interception, consumers would be reluctant to use emerging electronic media, such as cellular phones and e-mail, to communicate. The resulting law extended legal protection akin to that provided First Class mail, and was developed and supported by a diverse coalition of business, civil liberties, and consumer advocates who understood that consumers would be unwilling to fully embrace electronic mail and other new technologies without strong privacy protections.

Similarly, the 1995 amendments to ECPA crafted privacy protections for transactional information that was content-like in its ability to reveal facts about a person's life. In these instances, developing and enacting a legislative privacy regime was viewed by the business community as a necessary component of creating and supporting a flourishing market for their products. The nexus between privacy protection and business necessity resulted in a diverse public interest/industry coalition supporting increased protections for transactional data. Communications Assistance and Law Enforcement Act of 1994, Pub. L. No. 103–414, § 207, 108 Stat. 4279 (codified at 18 U.S.C. §§ 2510—2711 (1994)). There is dispute over whether other sections of CALEA solve or create privacy problems.

Other privacy legislation supported by the public and private sectors The Cable Communications Privacy Act of 1986 and the Video Privacy Protection Act of 1988 reflect a similar coalescing of interests. Enacted within a couple of years of each other, both laws resulted from the affected industry's realization that a lack of assurance that viewing preferences were protected from prying eyes, would have a chilling effect on consumers' viewing and renting habits. The revelation in a Washington, DC, weekly paper, that a reporter,—or anyone for that matter—could walk in off the street and discover Supreme Court nominee Judge Bork's taste in movies provided privacy advocates with the perfect story to gain Congress's attention. Privacy advocates arrived on the Hill with Erols, the Video Software Dealer's Association, the Direct Marketing Association, and others who realized that the viability of their businesses depended on consumer trust and confidence that video rental lists were safeguarded by strong legal restrictions on government and private sector access.

In other instances, industry has been moved to support privacy legislation in the wake of public revelations of bad practices or a particularly compelling horror story. The Fair Credit Reporting Act of 1970 ("FCRA") was initially drafted and supported by the credit reporting industry in response to congressional hearings which revealed widespread misuse of credit

Today, the dialogue over assuring privacy on the Internet and in electronic commerce is well situated for a successful legislative effort. Privacy-aware companies are seeking to develop and implement self-regulatory programs. Surveys have shown that the viability of online commerce depends upon the existence of real protections for consumers' privacy. Similar to the development of early privacy laws, some industry actors have led the way crafting self-regulatory policies that are the prototype for subsequent legislation supported by self-regulated players who for reasons of public trust, liability, and/or government concern want to bind bad industry actors.

Advocates of both self-regulation and legislation each have a vested interest in exploring and resolving the hard issues. Questions of what is personally identifiable information in the context of the Internet, what does access require, and what is the appropriate way to police and provide remedies in this environment must all be explored. The work of the Online Privacy Alliance to develop principles to protect children's privacy became a starting point for the recently passed Children's Online Privacy Protection Act.[77] The collective desire to provide privacy protections that protect individuals' privacy, and encourage them to participate in the online environment, provides the common ground for the development of sound policies and enforcement strategies in the coming year.

E. *Create a Privacy Protection Entity to Provide Expertise and Institutional Memory, a Forum for Privacy Research, and a Source of Policy Recommendations on Privacy Issues*

The work outlined above, and the state of privacy today, all weigh in favor of creating a privacy entity within the federal government. The existing approach has hindered the development of sound policy and failed to keep pace with changes in technology. The United States needs an independent voice empowered with the scope, expertise, and authority to guide public policy. Such an entity has important roles to play on both

---

information and an alarming rate of inaccuracies in credit reports. An enraged Congress, with the support of privacy and consumer organizations, indicated a commitment to passing a law regulating the use of consumer credit information. Realizing that legislation was inevitable, the industry set about crafting a policy that they could support. The Driver's Privacy Protection Act of 1994 was largely triggered by the murder of actress Rebecca Shaffer and eventually garnered the support of the majority of the affected industries. Through information in her driver license file at the department of motor vehicles, Shaffer's stalker was able to learn her whereabouts.

77. The Privacy Act of 1974, 5 U.S.C. § 552a (1973).

domestic and international fronts. It would serve as the forum for collaboration with other governments, the public interest community, and the business community.

There are a myriad of functions an entity charged with promoting privacy could perform. Unfortunately, the debate over the scope and power of such an agency or office has consistently stymied attempts to create one. As in many areas, the perfect has been the enemy of the good. At this junction, foremost on this entity's agenda should be developing and articulating a comprehensive vision of privacy protection for the United States, and coordinating efforts to advance it in both the public and private sector. The emergence of the Internet and other advanced technologies require us to reflect, study, adapt, and apply existing privacy principles and at times develop new ones. Without expertise and devoted resources this task will not be undertaken.

To function well, such an entity should have the ability to

1. monitor and evaluate developments in information technology with respect to their implications for personal privacy;
2. conduct research, hold hearings, and issue reports on privacy issues in both the public and private sector;
3. develop and recommend public policy appropriate for specific types of personal information systems;
4. comment upon government and private sector proposals that impact on privacy;
5. review agency activities under the Privacy Act;
6. participate in government proposals that impact on privacy.[78]

The level of 1) public concern; 2) agency activity; 3) private sector investment; and 4) non-governmental organization focus on individual privacy, cry out for the formation of an entity able to comprehensively and effectively address privacy issues.

In July, Vice President Gore announced the Administration's intent to appoint an individual to oversee and coordinate the governments privacy

78. A number of these recommendations mirror those made by Flaherty in his recommended responsibilities for a United States privacy protection commission. He goes on to state that such a commission should have a statutory mandate and as much independence as possible from the executive and legislative branches of government. (source on file with author).

activities as part of the "Electronic Bill of Rights."[79] While the duties and powers of this individual are unclear, the announcement signals the Administration's recognition that privacy is an issue of growing importance and one that the Administration must play a role in coordinating. As of publication, no appointment has been made.

F. *We Must Question Our Tendency to Rely on Government as the Central and Sometimes Sole Protector of Privacy*

In the decentralized and global environment of the Internet, the law's impact will be limited. In an area such as privacy, where the government's actions have often been detrimental rather than supportive, we must ask if other options—such as technology may provide stronger protection. We must encourage the development and implementation of technologies that support privacy. They are critically important on the Internet and other global medium. Strong encryption is the backbone of technological protections for privacy. Today technical tools are available to send anonymous e-mail, browse the World Wide Web anonymously, and purchase goods with the anonymity of cash.

Public policy is quickly becoming as much a product of computer code and product decisions as law. Advocates who once focused nearly exclusively on federal and state legislatures and agencies are increasingly seeking to influence the design of technical standards and specifications, and even specific product designs. From the Internet Engineering Taskforce and the World Wide Web Consortium, to the United States Telephone Association, decisions that will affect the future of privacy are made each day. Advocates, the public, and policy-makers have taken fire at specific products ranging from Lexis-Nexis Ptrak[80] to the soon to be released Intel Pentium III Processor seeking to ward off privacy invasions. But as we ward off the bad, we must move for the development of the good—seeking to foster technologies,—both standards and specific products,—that protect privacy.

Future technical developments have the capacity to provide an underlying framework for privacy, providing greater anonymity, confidentiality, and a platform for fair information practices.[81] Technologies

---

79. *Vice President Gore Announces New Steps Toward an Electronic Bill of Rights* Presswire, July 31, 1998, at 1, *available in* 1998 WL 16515766.

80. *See supra* Part IV.

81. These incorporate the basic concepts of three recommendations of the Danish and Canadian Privacy Commissioners: 1) eliminate the collection of identity information, or if it is needed, keep it separate from other information; 2) minimize the collection and retention of identifiable personal information; and 3) make data collection and use transparent to data subjects

must be a central part of our privacy protection framework, for they can provide protection across the global and decentralized Internet where law or self-regulation may fail us.

V. CONCLUSION

No doubt, privacy on the Internet is in a fragile state, however, there is new hope for its resuscitation. The business community, enlightened by survey upon survey documenting consumers' privacy concerns, has recently begun serious efforts at self-regulation. The White House, the Federal Trade Commission, the Department of Commerce, and Congress all show interest in ensuring that privacy is protected as the digital economy is embraced. A growing number of advocacy organizations, ranging from consumer to civil liberties to libertarian organizations, have begun to focus on privacy. Thanks to the Internet, the public voice is being heard more clearly than ever—more often than not weighing in strongly in support of privacy protections through law and technology.

There is a special need now for dialogue. Providing a web of privacy protection to data and communications as they flow along networks requires a unique combination of tools—legal, policy, technical, and self-regulatory. Cooperation among the business community and the nonprofit community is crucial. Whether it is setting limits on government access to personal information, ensuring that a new technology protects privacy, or developing legislation—none will happen without a forum for discussion, debate, and deliberation.

---

and provide them with the ability to control the disclosure of their personal information, particularly identity information. *See supra* Part IV.

Amelia H. Boss
Professor Temple University, School of Law

Amelia H. Boss, a graduate of Bryn Mawr College and Rutgers-Camden Law School, is a Professor of Law at Temple University School of Law, where she teaches in the commercial law, bankruptcy, and electronic commerce areas. She is a member of the Permanent Editorial Board of the Uniform Commercial Code, and the former chair of the Uniform Commercial Code Committee of the American Bar Association. She serves as the American Law Institute member of the Drafting Committee to revise Article 2 of the UCC on sales, of the Drafting Committee on the new Article 2B on licensing of software, and of the Drafting Committee to revise Article 1 on general provisions. In the past, she served as an advisor/observer to the revisions on Article 5 (letters of credit) and Article 8 (investment securities). She is a member of the American Law Institute and served on the Members Consultative Group on the Restatement of the Law of Suretyship. Professor Boss is a member of the Council of the Section of Business Law of the American Bar Association, and will assume the role of secretary of the section in August. She is a member of the former fellow of the American College of Commercial Financial Lawyers and is a member of the Board of Directors of the Institute of International Commercial Law.

Professor Boss currently serves as advisor and as the United States Delegate to the United Nations Commission on International Trade Law (UNICITRAL) on issues relating to electronic commerce. She represented the U.S. in the development of the UNCITRAL Model Law on Electronic Commerce, and is now representing the U.S. in UNCITRAL work on digital signatures. She serves as the American Bar Associations representative to an effort by the National Conference of Commissioners on Uniform State Laws to draft a Uniform Electronic Commerce Act, dealing with *inter alia* with digital signatures. She is Editor-in-Chief of *The Data Law Report* (published bi-monthly by Clark Boardman Callaghan), is on the editorial board of *The EDI Law Review* and the *Journal of Bankruptcy Law and Policy*, and is the editor of the new book series, *ABC's of the UCC*, published by the American Bar Association.