ARTICLE

TRANSLATING PRIVACY VALUES WITH TECHNOLOGY

SHAWN C. HELMS*

* Shawn C. Helms is an attorney in the Information Technology practice group of Cooley Godward LLP and is the former Director of Information Technology at the law firm of Williams & Connolly LLP. The author would like to thank the staff of the *Boston University Journal of Science & Technology Law*, Debra Ashley, Jason Conger, Scott Graziano, Misty Helms, and Natalie Holick for their efforts on this article. The author would like to give special thanks to Professor Julie E. Cohen of Georgetown University Law Center for her critiques, edits, insights and inspiration.

I. INTRODUCTION

In 1890 Louis Brandeis said that all Americans have "the right to be let alone. . . ."[1] In many ways this often-quoted privacy mantra was a statement of a value more than a statement of a legal right. One has no legally protected overarching "right" to privacy,[2] yet Americans value their privacy and sometimes go to great lengths to protect it.[3] In many ways, the ability to conduct one's daily activities beyond the prying eyes of government or other citizens has come to be a necessary component of civilized society.[4] The totalitarian idea of "Big Brother" monitoring one's every move invokes fear and sometimes emphatic responses from Americans.[5] Privacy, as a simple concept of integrity, has inspired societies to create laws against invasive actions such as stalking, wiretapping, and unreasonable government searches.

However, where society has attempted to protect, technology has attacked. Despite a number of new laws,[6] constitutional interpretations, and private self-regulation, technology has eroded privacy at a rapid rate. In 1890, Brandeis was alarmed by photography, a new technology that he viewed as a serious threat to personal privacy.[7] Today, the new technology threatening privacy is

---

[1] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890) (establishing the broad parameters of the right to privacy as the right to be let alone).

[2] Although the Supreme Court has not recognized an absolute right to privacy, it has found some limited constitutionally protected rights to privacy. *Compare, e.g.*, Bowers v. Hardwick, 478 U.S. 186, 190-91 (1986) (rejecting a constitutional right to engage in homosexual sodomy in the privacy of one's home), *with* Roe v. Wade, 410 U.S. 113, 152-53 (1973) (finding a constitutional zone of privacy in a "woman's decision whether or not to terminate her pregnancy"), *and* United States v. Karo, 468 U.S. 705, 714 (1984) (holding that government monitoring of a beeper signal emanating from an individual's home violates the individual's privacy interest in his home).

[3] For example, we build high fences around our yards and pay for private rooms in hotels.

[4] Election by secret ballot, Alcoholics Anonymous, and unlisted phone numbers are just a few examples of how privacy and the ability to remain anonymous has been institutionalized into our society.

[5] The Big Brother analogy comes from Orwell's 1949 novel *Nineteen Eighty-Four*. *See generally* GEORGE ORWELL, NINETEEN EIGHTY-FOUR (Oxford Univ. Press 1984) (1949).

[6] Since 1970, Congress has enacted several laws to protect individual privacy from information collection and monitoring enabled through computer systems. *See* Privacy Act of 1974, 5 U.S.C. § 552a (1994 & Supp. V 2000); Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (1994 & Supp. IV 1999); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (1994); Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 (1994); Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2703 (1994).

[7] *See* Warren & Brandeis, *supra* note 1, at 195 (noting the call for a law to "remedy . . .

the computer.

Computer databases, hardware, software, and network standards are facilitating the identification of individuals in order to increase the efficiency of communication and commerce. The Internet is, by definition, a single network, and poses significant potential for large scale and detailed monitoring that has never before been possible. The development of identification technology and detailed tracking is also being supported by political, legal, and market forces, which are moving us toward a surveillance-based society. These technological and societal developments pose a serious threat to an individual's anonymity and personal privacy.

The purpose of this article is to explore anonymity, its value to society, and how best to protect this value in cyberspace. This article argues that the ability to remain anonymous is essential in a free society and that, without full appreciation of the consequences, we are losing privacy through the advancement of identification technologies. To counter the anti-privacy aspects of technology, scholars, policy makers, and industry have suggested a number of approaches, including constitutional interpretations, common law privacy torts, legislation, and market based self-regulation through privacy policies. Despite these efforts, no workable solution has arisen for protecting anonymity on the Internet. This is primarily due to: (1) legal, political, and market forces that favor commerce, law enforcement, and accountability; and (2) a market for privacy that, while still in its infancy, is being retarded in its development by a powerful market for identification technology.

This article examines these realities and proposes that anonymity on the Internet can only be achieved by building a market for privacy that will implement privacy-enhancing technologies (PETs). Simply put, the government, privacy advocacy groups, software companies, and individual users should develop, use, promote, and advance privacy education and the adoption of PETs that allow for anonymity over the Internet. While this approach has a number of potential problems, this article submits that it is the best method of continually enabling anonymity within a changing technological world.

To focus the discussion, Part II of this article looks at technological developments on the Internet that challenge one's ability to remain anonymous. Such technologies are moving us toward a "Cyber-Panopticon" and posing a serious challenge to those whom wish to remain anonymous. Part III explores the relationship between privacy and anonymity. Part IV looks at the current legal structures that attempt to protect personal privacy. Part V discusses the specifics of PETs, and attempts to show that: (1) there is currently little political or market force pushing for the protection of anonymity, and that, in fact, the opposite is true; (2) anonymity is nevertheless important, and PETs should therefore be developed to enable anonymous communication over the Internet; and (3) the government, privacy advocacy groups, technology companies, and individual users must proactively work for the wide adoption of PETs. Part VI concludes that if society does not adopt PETs, the Internet will become a medium of persistent identification, thus

---

the unauthorized circulation of portraits of private persons").

undermining basic privacy values that are important in a free society.[8]

II. THE TECHNOLOGICAL TREND TOWARD THE CYBER-PANOPTICON

A. The Cyber-Panopticon

For better or for worse, technology is undoubtedly the most potent change agent in society today. Technological advancements are altering the way we interact with businesses, schools, governments, and each other. Through technology we can accomplish tasks with startling efficiency and perform others that were once thought impossible. Many technological changes, however, create unforeseen consequences that cut against values society seeks to protect. Society often does not realize these consequences until after it has implemented the technology.[9] The Internet has raised a number of such unforeseen problems,[10] including what many view as serious privacy concerns.

Long before the Internet was conceived, Jeremy Bentham envisioned a physical structure designed to eliminate privacy. He called this structure the Panopticon.[11] Bentham imagined prison cells built in a circle around a guard tower, with light coming through windows on the outside of the cells.[12] Such a design would silhouette each prisoner, thus making it easy for a single guard to monitor a large number of convicts.[13] Bentham and others recognized that such a system would be an effective control even if no guard occupied the tower.[14] "The very fact of general visibility – being see*able* more then being seen – will be enough to produce effective social control."[15]

With Bentham's schematic in mind, computer and communication technology can be appropriately classified as the "Cyber-Panopticon." Computer and communication technology has enabled monitoring of personal activities with an amazing amount of specificity. Consider a few such technologies and systems: database records track credit card purchases,

---

[8] On a very basic level, some authors have equated privacy to freedom. *See* Robert S. Peck, *The Right to Be Left Alone*, 15 HUM. RTS. 26, 27 (1987) ("Privacy makes possible individuality, and thus, freedom.").

[9] There are numerous examples of safety hazards surfacing only after society implements new technology. *See, e.g.*, Pete Donohue, *Danger Merges at Toll Plazas: E-Zpass Speedsters Cause Rise in Accidents,* DAILY NEWS (N.Y.), Aug. 21, 2000, at 17 (noting increased accidents at toll booths that use E-Z Pass scanners), *available in* LEXIS, News Library, Dlynws File; Phil Frame, *Child Airbag Deaths Spark Recommendations for Preventive Measures,* AUTOMOTIVE NEWS, July 29, 1996, at 8 (noting an increase in child deaths from airbags), *available in* LEXIS, News Library, Autonw File.

[10] Many of our legal and social structures have been challenged by the rise of the Internet, including traditional taxation, legal jurisdiction, protection of intellectual property, export controls, and regulation of speech.

[11] *See* Jeffrey H. Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future,* 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 27, 28 (1995) (discussing Bentham's Panopticon structure).

[12] *See id.*

[13] *See id.*

[14] *See id.*

[15] *Id.*

telephone calls, and items purchased in a supermarket.[16] Mobile telephone companies install tracking mechanisms to pinpoint the location of active mobile phones.[17] Electronic tollbooths and traffic monitoring systems record the movement of individual vehicles.[18] Closed circuit TV cameras monitor city streets and college dorm rooms.[19] Intelligent software systems identify individuals from video images.[20] DNA databases store biological blueprints of thousands of people.[21] Electronic key systems monitor entry and exit from buildings.[22] Biometric technology identifies people from their voices, retinas, or fingerprints.[23] Tiny microphones record conversations from considerable distances by detecting the vibrations of window glass.[24] "Smart homes" monitor usage of doors, appliances, lights, and other utilities.[25] Personal identification cards store medical and credit history, data on physical characteristics, and private encryption keys allowing for foolproof digital signatures.[26]

Often such identification and monitoring technology is used for facially legitimate purposes, such as fighting crime, increasing efficiency in commerce, assisting public safety, delivering better healthcare, and saving time. Each of these technologies, however, adds to the Panopticon's circle yet another lighted cell through which people can be observed. These technologies are moving us toward a society in which our every action is monitored and electronically recorded for posterity.

If monitoring technologies are the lighted cells in the Panopticon, the

---

[16] *See, e.g.*, Steven E. Brier, *Smart Devices Peep Into Your Grocery Cart,* N.Y. TIMES, July 16, 1998, at G3 (discussing technologies used by supermarkets that can track consumer purchases).

[17] *See, e.g.*, Simon Romero, *Location Devices' Use Rises, Prompting Privacy Concerns*, N.Y. TIMES, Mar. 4, 2001, at 1.

[18] *See, e.g.,* Abdon M. Pallasch, *Big Brother On Road,* CHI. SUN-TIMES, Dec. 8, 1999, at 1, *available in* LEXIS, News Library, Chisun File.

[19] *See, e.g.*, Christopher S. Milligan, Note, *Facial Recognition Technology, Video Surveillance, and Privacy,* 9 S. CAL. INTERDISC. L.J. 295, 300-03 (1999).

[20] *See id.* at 304.

[21] *See, e.g.,* Michael Hedges, *Backlogs Keep DNA Evidence on Shelf,* PLAIN DEALER, Feb. 29, 2000, at 8A, *available in* LEXIS, News Library, Clevpd File.

[22] *See, e.g.*, Richard Burnett, *Security Technology Has Lock on Future,* ORLANDO SENTINEL TRIB., Feb. 5, 1996, at 14, *available in* LEXIS, News Library, Orsent File.

[23] *See, e.g., id.*; Michael Bartlett, *Companies Promise Biometric Security for E-Business,* NEWSBYTES, Feb. 21, 2001, *available at* <http://www.newsbytes.com/news/01/162257.html>.

[24] *See*, *e.g.,* James Gerstenzang, *Keeping Things Up to Date in Kennebunkport,* L.A. TIMES, Aug. 28, 1990, at H3 (discussing surveillance technology used in protecting then-President George Bush, Sr.), *available in* LEXIS, News Library, Lat File; Nathaniel Sheppard Jr., *Technology Favors 'Bugs' Over Security*, CHI. TRIB., Apr. 12, 1987, at 14 (discussing advances in eavesdropping technology), *available in* LEXIS, News Library, Chtrib File.

[25] *See, e.g.,* Thomas A. Fogarty, *'Smart Homes' Becoming Reality,* DES MOINES REG., May 16, 2000, at 3, *available in* LEXIS, News Library, Dmoirg File.

[26] *See, e.g.*, Alan S. Horowitz, *Smart Cards in Every Wallet? Maybe*, PLANET IT, Oct. 27, 2000, *available at* <http://www.PlanetIt.com/docs/PIT20001031S0018>.

Internet is the centralized guard tower. Because the Internet is a worldwide network, it can connect, coordinate and centrally aggregate all privacy invading technologies.[27] The Internet is becoming the medium of choice for a significant portion of society's communication and commerce. The Internet combined with identification technologies is leading us toward the Cyber-Panopticon, where one's every move can be monitored in real-time, stored in electronic form, and later analyzed with granular particularity. Like the guard tower, the Internet may be the most important piece of this technological trend toward a Cyber-Panopticon.[28]

B. Internet Identification Technology

As the Internet matures, hardware and software engineers are developing an increasing number of methods to identify individual users. These identification methods threaten one's ability to remain anonymous on the Internet. Anonymity and the fear of "Big Brother" tracking one's every move on the Internet have received significant attention from scholars.[29] Some scholars believe that the Internet should be a platform for anonymous communication, a completely uninhibited forum for free expression.[30] Others are concerned that absolute anonymity will paralyze law enforcement[31] as nefarious activity proliferates because officials will be unable to identify and therefore hold accountable culpable parties.[32]

---

[27] Other scholars have theorized that the Internet could be used as a platform for centralized social monitoring and control. *See, e.g.*, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE xi-xx, *passim* (2d ed. 1999). Lessig described the views of science fiction writers Vernor Vinge and Tom Maddox, who in 1996 saw the Internet as the platform for a "perfectly ordered network of control." *Id*. at x. Lessig goes on to say that at the time of Vinge's and Maddox's statements, "[e]nvisioning this impossible world was sport. Now the impossible has been made real. Much of the control in Vinge's and Maddox's stories that struck many of their listeners as Orwellian now seems quite reasonable." *Id.*

[28] Even if one does not agree with this alarmist view of the Cyber-Panopticon, the numerous and novel monitoring and information compiling technologies accessible through the Internet provide a useful frame of reference to carefully consider technology's impact on basic privacy values.

[29] *See generally* Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639 (1995); A. Michael Froomkin, *Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395 (1996); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998); LESSIG, *supra* note 27; Lee Tien, *Who's Afraid of Anonymous Speech?* McIntyre *and the Internet*, 75 OR. L. REV. 117 (1996); Myrna L. Wigod, *Privacy in Public and Private E-Mail and On-Line Systems*, 19 PACE L. REV. 95 (1998); Donald J. Karl, Comment, *State Regulation of Anonymous Internet Use After* ACLU of Georgia v. Miller, 30 ARIZ. ST. L.J. 513 (1998).

[30] *See, e.g.*, Tien, *supra* note 29, at 120, 122 (arguing that online anonymity protects self-identity).

[31] In this context, I am using "law enforcement" to connote "public and private enforcement mechanisms." David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, 1996 U. CHI. LEGAL F. 139, 142 (1996).

[32] *See* Branscomb, *supra* note 29, at 1642-43 ("[Anonymity] often encourages

The popular press also has focused on the issue of anonymity over the Internet. In early 1999, Intel Corporation announced that it planned to embed Processor Serial Numbers (PSNs) in its Pentium III microprocessors.[33] PSNs can identify individual machines and transmit the information to Internet servers.[34] Such desktop level identification invoked Orwellian-like concerns with some privacy groups and members of the public.[35] Other commentators, however, were troubled at law enforcement's lack of recourse when several major commercial web sites, including Yahoo!, eBay, and E-Trade, were attacked by anonymous hackers.[36] As the Internet expands, the tension between the virtues espoused by anonymity, and the problems that occur because of it, will only grow.

According to one recent statistic, 122 million Americans regularly use the Internet to communicate or find information.[37] While using the Internet, a number of technical realities conspire to associate an individual's Internet actions with their biological identity, thus preventing anonymous communication. In most instances, these technological methods of identification can be countered with PETs that can protect one's anonymity.[38]

1. TCP/IP Address

The Internet is a worldwide network of computers; these computers exchange information in a common language or protocol called TCP/IP.[39] To communicate on the Internet, every computer must have a TCP/IP address. A TCP/IP address is either dedicated to a computer (a static TCP/IP address) or is dynamically assigned to an individual's computer, at the time of access, by a service provider that facilitates Internet communication. A global, coordinating organization distributes a range of TCP/IP addresses to Internet Service Providers (ISPs) and other organizations that connect directly to the

---

outrageous behavior without any opportunity for recourse to the law for redress of grievances."); George P. Long, III, Comment, *Who are You?: Identity and Anonymity in Cyberspace*, 55 U. PITT. L. REV. 1177, 1179 (1994) ("[A]nonymity . . . will discourage users from taking responsibility for their own communications," thus "effectively encourag[ing] the posting of illegal and abusive messages to the Net.") (citations omitted); Walter S. Mossberg, *Accountability is Key to Democracy in the On-Line World*, WALL ST. J., Jan. 26, 1995, at B1 ("[Anonymity] makes it easier to spread wild conspiracy theories, smear people, conduct financial scams or victimize others sexually.").

[33] *See* Frank James, *Intel Chip Fires up Privacy Debate*, CHI. TRIB., Jan. 22, 1999, at 1, *available in* LEXIS, News Library, Chitrib File.

[34] *See id.*

[35] *See, e.g.*, *Intel to Drop PSN in New Chips!*, BIG BROTHER INSIDE, Apr. 28, 2000 (encouraging consumers to boycott Intel products that use Processor Serial Numbers), *available at* <http://www.bigbrotherinside.com>.

[36] *See* David P. Hamilton, *Making Net Less Vulnerable Not an Easy Task*, CHI. TRIB., Feb. 21, 2000, at 5, *available in* LEXIS, News Library, Chitrib File.

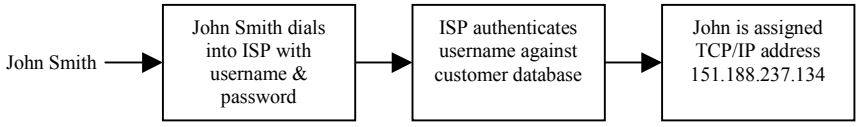
[37] *See Coming to Grips With the World Wide Web*, N.Y. TIMES, Dec. 11, 2000, at C1.

[38] Given the current market, however, privacy enhancing technologies ("PETs") may not be a viable solution for novice computer users. *See infra* Part V.

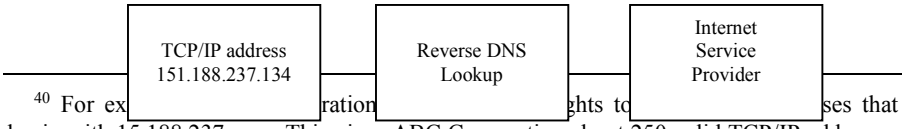
[39] TCP/IP stands for Transmission Control Protocol/Internet Protocol. TCP/IP is the core language of the Internet. A TCP/IP address is a numerical address consisting of 4 octets (*e.g.*, 151.188.237.134).

Internet.[40] Because of this centralized distribution process, a TCP/IP address can be tracked to the specific organization to which it was assigned.

Most Internet users are not continually connected to the Internet.[41] Instead, the average Internet user accesses the Internet through a modem and a dialup ISP account.[42] The modem dials across a telephone line to an ISP and creates a temporary connection. After the modem connects with the ISP computer, the user is prompted for a username and password. The username and password are linked to detailed personal information in the ISP's customer database. The ISP uses the username and password to verify that the user has an account with the ISP.[43] Once the account information is authenticated, the ISP assigns the dialup user one of the ISP's assigned TCP/IP addresses.



Address assignment can be used to identify an online user. The TCP/IP address is exchanged with every system with which the user interacts.[44] Through a method called a reverse DNS look-up, TCP/IP addresses return the identity of the ISP to which it was assigned; subsequently, one can identify the user by way of the ISP's customer information database.[45]



[40] For ex ration ghts to ses that begin with 15.188.237.xxx. This gives ABC Corporation about 250 valid TCP/IP addresses that can be assigned to computers within ABC Corp. Any communication that originates from a TCP/IP address beginning with 151.188.237 likely comes from ABC Corporation.

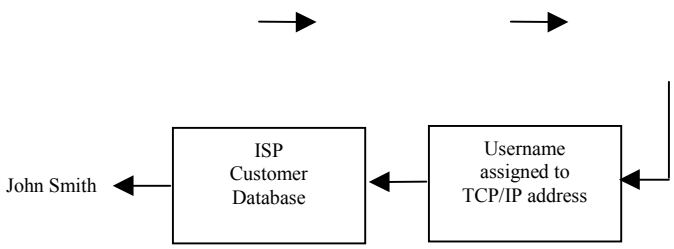
[41] *See* Julian Epstein, *A Lite Touch on Broadband: Achieving the Optimal Regulatory Efficiency in the Internet Broadband Market*, 38 HARV. J. ON LEG. 37, 43 n.35 (2001). Some users who connect to the Internet via a cable modem, DSL or corporate network have a static TCP/IP address and are continually connected to the Internet.

[42] *See id.* As of April 2001, the world's largest ISP, America Online, has almost 30 million customers. *See Worldwide AOL Membership Surpasses 29 Million*, AOL TIME WARNER, Apr. 16, 2001, *available at* <http://media.aoltimewarner.com/media/press_view.cfm?release_num=55251842>.

[43] ISPs track the exact time subscribers are online, thus helping to pinpoint online activity.

[44] *See Privacy Analysis of Your Internet Connection*, PRIVACY.NET (showing the information a Web site can obtain about a system, including TCP/IP address, ISP, the type of Internet browser used, and the last Web site visited), *available at* <http://privacy.net/anonymizer>.

[45] Domain Name System (DNS) translates host names (*e.g.*, aol.com) into TCP/IP addresses (*e.g.*, 143.123.165.170). One can look up the host name associated with a TCP/IP address using the WHOIS database at Network Solutions. *See WHOIS*, NETWORK SOLUTIONS, INC., *available at* <http://www.networksolutions.com/cgi-bin/whois/whois>. One can even find the longitude and latitude for an IP address. *See Host Name to Longitude/Latitude*, *available at* <http://cello.cs.uiuc.edu/cgi-bin/slamm/ip2ll>.



Through this process, one only needs the TCP/IP address and a cooperative ISP to link online activity to a user's biological identity.[46]

[46] One caveat to this example is that entire families often share one Internet account, or people allow a friend to use their username and password. In these instances, the TCP/IP address and username would not directly identify the specific user, but would provide some information toward identifying the online actor.

2. Email Domain Name

Determining the origin of an email is also a simple process. By looking at an email address, one may potentially gain both the ISP information and the individual's username. For example, "johnsmith@aol.com" clearly identifies America Online (aol.com) as the originating ISP and johnsmith as the originator's username.[47]

As with the TCP/IP example, the ISP uses the username to verify the user's account. The ISP often has detailed personal information concerning that username including name, address, phone number, and credit card information. Law enforcement and other entities can request or compel this information from ISPs, thus leading to identification of Internet users.[48]

3. Cookies

Computer files called cookies can also expose the identity of Internet users.[49] World Wide Web servers generate cookie files and store them on a user's computer for future Web server access.[50] Cookies allow Web servers to recognize the user's browser, provide the user with customized content, and store information about the user.[51] Often, users do not notice this storage and access of personal information because Web servers automatically access cookies whenever the user connects to the Web server.[52]

Without overt disclosure on the user's part, cookies generally do not reveal the biological identity of a user, and cannot be used to determine other sites the user has visited.[53] There are, however, two potential ways in which a cookie can be used to discover a user's identity. First, cookies can be used to recall authentication or login information (*e.g.*, name, address, password, etc.) that suggests the user's identity.[54] The user must first disclose the identifying information on the Web site for a cookie to include this type of identifying information. Second, an organization can cross-reference the information in a

---

[47] Even if an address has a little known domain name (*e.g.*, johnsmith@smallco.com), one can find the contact information of this ISP (smallco.com) by querying the WHOIS server. *See supra* note 45.

[48] *See* McVeigh v. Cohen, 983 F. Supp. 215, 217, 222 (D.D.C. 1998) (enjoining United States Navy from taking adverse action against plaintiff, whom the Navy had sought to discharge after AOL disclosed his identity in connection with a username that suggested he was homosexual).

[49] *See generally* Viktor Mayer-Schönberger, *The Internet and Privacy Legislation: Cookies for a Treat?*, 1 W. VA. J.L. & TECH. 1.1 (1997) (discussing cookie technology and its impacts on privacy), *available at* <http://www.wvu.edu/~wvjolt/Arch/Mayer/Mayer.htm>.

[50] For more an extended explanation of cookie technology, see Eamonn Sullivan, *Are Web-based Cookies a Treat or a Recipe for Trouble?*, ZDNET.COM, June 26, 1996, *available at* <http://www.zdnet.com/eweek/reviews/0624/24cook2.html>.

[51] *See id.* Cookies are used to store settings for customized search engines like My.Yahoo.com and to keep track of a shopping list at online stores like Amazon.com.

[52] *See* Mayer-Schönberger, *supra* note 49.

[53] *See* Sullivan, *supra* note 50.

[54] *See id.*

cookie with names, addresses and consumer histories that exist in marketing databases.[55] The Internet advertising firm DoubleClick, which acquired a massive marketing database through its purchase of Abacus Direct, proposed such a method of user identification last year.[56] While DoubleClick's plans for this combined database have been put "on hold," similar systems are sure to arise in the future.[57]

4. Processor Serial Number

In early 1999, Intel, the world's largest manufacturer of microprocessors, announced that it planned to include in its Pentium III chip a unique Processor Serial Number (PSN) that could identify a computer across the Internet.[58] According to Intel, it intended users to employ the linking of a PSN to the user's real world identity for authentication purposes in electronic commerce.[59] Intel would likely link the information through a registration process in which it would log into a database the user's personal information in conjunction with his or her PSN. This database could then be accessible to companies doing business over the Internet.

Such a system would greatly reduce the information-gathering burden on e-commerce companies who today must collect personal information from each user who purchases from their site. For example, if a user wants to purchase a book from Amazon.com, he or she must register with the site and provide personal information including name, address, telephone number, and email address.[60] If the user was first registered in the PSN database, Amazon.com could eliminate the registration step by pulling the necessary personal information from the PSN database. This would not only increase the speed and efficiency of online transactions, but would also likely encourage online users to shop a wider range of sites. This behavior is currently discouraged by site based registration.[61]

As for its impact on anonymity over the Internet, the PSN raises novel threats.[62] Even before its release, the possibility of such a system in a home

---

[55] *See* John Buskin, *Our Data, Ourselves*, WALL ST. J., Apr. 17, 2000, at R34.

[56] *See id.*

[57] *See* Fred Vogelstein, *Minding One's Business: Under Fire, DoubleClick Shelves Online Ad Project*, U.S. NEWS & WORLD REPT., Mar. 13, 2000, at 45.

[58] *See* James, *supra* note 33.

[59] *See id*.

[60] *See generally* <http://www.amazon.com>.

[61] For example, if a user is registered at BlueLight.com and knows the price and selection is comparable to that available at WalMart.com, the user might not ever shop at WalMart.com. Furthermore, even if the user knows that a product is one dollar cheaper at WalMart.com, the user still might chose to buy from BlueLight.com because he or she knows it would take time to register at WalMart.com.

[62] This year Intel announced that it would not include the PSN in the Pentium 4 microchip. *See* Robert Lemos*, Intel Disables ID Tracking In New Chips,* ZDNET INTERACTIVE WK., Apr. 27, 2000, *available at* <http://www.zdnet.com/intweek/stories/news/0,4164,2556671,00.html>; Robert O'Harrow Jr. & Elizabeth Corcoran, *Intel Drops Plans to Activate Chip IDs*, WASH. POST, Jan. 26, 1999, at E1.

computer had a dramatic impact on the Internet privacy debate.[63] For the first time, there existed a potential for identification technology to move from segmented ISPs to a centrally organized database that allowed organizations to track and log individual user's communications and actions. After an outcry by privacy advocates, Intel provided a software fix that professed to disable the PSN feature.[64] Shortly after this shutoff system became available, however, a computer expert at *C'T* magazine figured out how to remotely re-enable the PSN identification system without the user's knowledge and without the user having to reboot his computer.[65]

5. IPv6

IPv6, a proposed TCP/IP protocol for Internet communication, could be the nail in the coffin of anonymity on the Internet.[66] In response to concerns that the previous version of TCP/IP (IPv4) was running out of room to accommodate all of the individuals and networks that needed IP numbers, the Internet Engineering Task Force (IETF) developed the IPv6 protocol.[67] For the purposes of this article, the most important change from IPv4 to IPv6 concerns IPv6's authentication capabilities. Currently, the structure of IPv4 allows users to create false return addresses on data packets, thus making some communications virtually impossible to trace.[68] IPv6, by contrast, marks each packet with an encryption "key" that cannot be altered or forged, thus securely identifying the packet's origin.[69] This authentication function can identify every sender and receiver of information over the Internet, thus making it nearly impossible for people to remain anonymous on the Internet.[70]

The current plans for IPv6 also allocate a permanent address to every device on the Internet.[71] Currently, most IP addresses are only temporarily allocated to Internet users.[72] The new addresses of IPv6 "will be embedded in hardware, and include information that can be traced back to individual network interface cards."[73] This will be like a permanent cookie that can never be disabled. The U.S. government is supporting the adoption of IPv6 technology in order to

---

[63] *See supra* note 35 and accompanying text.

[64] *See* Lemos, *supra* note 62.

[65] *See* Christian Persson, *Pentium III Serial Number is Soft Switchable After All*, C'T NEWS, May 1999, *available at* <http://www.heise.de/ct/english/99/05/news1>.

[66] *See* Hamilton, *supra* note 36 (noting that IPv6 would "make it harder for the people perpetrating [hacker attacks] to be anonymous").

[67] IETF is a not-for-profit international standards body that develops many of the operational protocols needed for Internet functioning. *See Overview of IETF*, IETF.ORG, Jan. 29, 1999, *available at* <http://www.ietf.org/overview.html>.

[68] *See* Hamilton, *supra* note 36.

[69] *See id.*

[70] *See id*.

[71] *See Latest IP Prompts Net Privacy Fears*, COMPUTING, Oct. 28, 1999, at 14 [hereinafter *Latest IP*].

[72] *See id.* ("Current addresses are only temporary."); s*ee also supra* notes 39-41 and accompanying text.

[73] *Id.*

protect public safety; IPv6 could, for example, help it catch Internet hackers.[74] Such a system, however, could certainly erode, if not eliminate, Internet anonymity.

III. EXPLORING ANONYMITY

A. Anonymity and its Relationship to Privacy

Anonymity is a somewhat elusive term. It is often lumped together with privacy generally and is rarely defined with precision. To facilitate the discussion of anonymity over the Internet, this section is devoted to defining anonymity and exploring how anonymity relates to privacy.

Legal scholars often speak in broad terms when referring to privacy. Privacy envelops a wide range of topics relating to integrity, personal property, movement, sensibilities, and information.[75] This article concentrates on anonymity, a specific aspect of privacy. Anonymity's relationship to privacy is dependent, overlapping, and sometimes just semantic. Anonymity is not a subset of privacy; rather, it can be thought of as the perfect realization, or product of, privacy. If you have privacy, you do not necessarily have anonymity.[76] However, privacy is a prerequisite to anonymity. Unless actions are performed in private, they can never be anonymous. If someone writes a letter in private, and does not sign his name or disclose his identity through its

---

[74] *See* Sinead Carew, *Wiretapping Protocol Could Destabilise Network Security*, VNUNET.COM, Jan. 6, 2000, *available at* <http://manageit.vnunet.com/Analysis/104960>.

[75] Joseph Rosenbaum has attempted to capture the breadth of differing privacy concepts by dividing privacy into three categories:

1. Territorial Privacy: one's right to be physically left alone or undisturbed. Territorial privacy is exemplified in the legal principles of trespass, real estate, and national sovereignty. This view of privacy allows one to impose physical boundaries around one's proprietary space to avoid the interference of other people or their effects.

2. Personal or Individual Privacy: one's right to be free in movement and expression without either physical assault or harassment in a non-physical sense (e.g., sexual harassment, defamation, obscenity). This type of privacy is based on social and cultural norms, and is tied to the individual's perceived sense of dignity rather than concepts of property. Laws concerning stalking, obscenity, and discrimination are related to this privacy category.

3. Information Privacy: one's right to protect dignity or integrity by preventing the disclosure, distribution, use, and abuse of information about oneself. This category of privacy is based on the idea that an individual has the exclusive right to disclose, communicate, control, or retain as private or public his personal information. People desire control over their personal information, allowing its disclosure to some and not to others, thus enabling citizens to govern their personal interactions. This category of privacy has been the focus of much attention due to recent advancements in the areas of database and data warehouse technology, in conjunction with the proliferation of the Internet. As a result, this type of privacy is also called "database privacy."

See Joseph I. Rosenbaum, *Privacy on the Internet: Whose Information is it Anyway?,* 38 JURIMETRICS 565, 566-67 (1998).

[76] If a person checks into a hotel room with his real name he is not anonymous. However, he might still say he has a "private" room. "Private" here means that the person can lock the door to exclude others from invading his physical space.

content, the letter can be anonymous. Privacy enables anonymity and anonymity is privacy realized.

Anonymity is also a matter of degree. Perfect anonymity is the absence of information related to the source of an action. An anonymous message, for example, provides the recipient no information as to the message's originator.[77] "[I]f I am no less uncertain about the identity of the message originator after I receive the message than I was before, the message is an anonymous one."[78] Such perfect anonymity is *not* the definition utilized in this article. In a number of respects, perfect anonymity is an impossible extreme. Imagine a person receiving an "anonymous" letter in the mail. Even if the letter is unsigned, the content and form tell the recipient something about the author. For example, if the letter is typed the originator had access to a typewriter or printer. If the letter uses English words, the originator speaks English and is literate. If the letter has a U.S. postmark, it likely originated from this country. If the letter has the recipient's correct address and the contents have some relationship to his life, the originator obviously knows the recipient in some way. These aspects of the letter give the recipient information about the originator. Thus, by the definition above, the letter is not perfectly anonymous.

In a real sense, however, this letter *is* anonymous. It may be impossible for the recipient to ever identify the person from whom the letter came. This basic level of anonymity might be called "threshold anonymity." Threshold anonymity occurs when a person's actions cannot be observed, attributed, or discovered. This is not to say that no information exists about the originator. Rather, the originator's identity is not readily discoverable. For purposes of this article, anonymity is always to be understood as threshold anonymity.

As stated above, privacy is a prerequisite to achieving anonymity. Therefore, this article sometimes will discuss protecting privacy without drawing the extension to anonymity. However, the goal is always to protect anonymity and privacy is simply a necessary means to that end.

B. Anonymity vs. Responsibility

Anonymity is praised as a necessary component of free society on one hand,[79] but condemned as a vehicle for nefarious activity on the other.[80] Critics of anonymity claim that a person who can speak or act anonymously will act irresponsibly because there is no personal cost to his actions.[81] If a person cannot be identified, he cannot be held accountable by law enforcement

---

[77] *See* Post, *supra* note 31, at 149.

[78] *Id.* at 149.

[79] *See* Warren & Brandeis, *supra* note 1, at 196 (discussing one's right to personal privacy); *see also* Kang, *supra* note 29, at 1196 (citing Justice Brandeis as saying privacy is "'the most comprehensive of rights and the right most valued by civilized men'").

[80] *See* Branscomb, *supra* note 29, at 1642 (discussing "many valid reasons supporting prohibition of anonymity"); Long, *supra* note 32, at 1179.

[81] David G. Post extends this beyond the individual by noting the aggregate effect as the "attendant moral hazard problem: to the extent individuals can avoid internalizing the costs that their behavior imposes on others, widespread anonymity may increase the aggregate amount of harmful behavior itself." Post, *supra* note 31, at 142.

or others in society for his anti-social or illegal behavior.[82] Critics say anonymity thus distorts behavioral incentives by allowing the individual to benefit and effectively elude personal responsibility, while imposing the cost of his adverse behavior on society.[83]

Supporters of anonymity argue that unpopular speech and action will be suppressed if people cannot remain anonymous, thus stifling the free flow of ideas that is essential in a democracy.[84] This latter point is supported by anonymity's association with historic incidents where political actors with unpopular views benefited from the ability to remain anonymous.[85] The *Federalist Papers*, arguably this country's most influential political writings, were published under the veil of anonymity.[86] Anonymity is a method of allowing people to communicate and act without fear of retribution.[87] Consequently, ideas or information that might never have been disclosed can become part of the public dialogue.

In its most recent case dealing with anonymity, *McIntyre v. Ohio Elections Commission*, the Supreme Court named an overarching privacy interest as at least one reason for protecting anonymous political speech.[88] When the *McIntyre* Court identified anonymity as facilitating and protecting a privacy interest, the Court also acknowledged that anonymity was an effective tool for protecting and promoting the marketplace of ideas.[89]

In *McIntyre*, Justice Scalia's dissent emphasized the negative aspect of anonymity.[90] Similar to the commentators discussed above, Scalia notes that anonymity is often used to diminish, or eliminate, accountability.[91] Although this criticism is compelling in some instances, this aspect of anonymity is often elusive because one might also have valid reasons for wishing to remain anonymous. For example, if a person anonymously speaks out against a

---

[82] *See* Branscomb, *supra* note 29, at 1642-43.

[83] *See* Mossberg, *supra* note 32.

[84] *See* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 982 (1996) (discussing how digital copyright management, which allows monitoring of citizens' reading habits, is contrary to the values of free speech because it stifles intellectual exploration).

[85] *See* Froomkin, *supra* note 29, at 409 (explaining the Federalist Papers' influential role in the fight for anonymity); *see also* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 360-61 (1995) (Thomas, J., concurring) (noting that the Federalist Papers are evidence of the Framers' understanding that the First Amendment protects anonymity in political speech).

[86] *See McIntyre*, 514 U.S. at 360.

[87] For example, without anonymity one might be hesitant to be tested for HIV, to purchase pornographic material, to practice an obscure religion, or to give "whistleblower" information to the police.

[88] 514 U.S. at 341-42 ("The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a *desire to preserve as much of one's privacy as possible*.") (emphasis added).

[89] *See id.* at 342.

[90] *See id.* at 381 (Scalia, J., dissenting) ("The silliness that follows upon a generalized right to anonymous speech has no end.")

[91] *See id.* at 385 (Scalia, J., dissenting) ("[E]liminating accountability . . . is ordinarily the very purpose of the anonymity.").

powerful organization, he might not want to take "responsibility" for the speech or personally defend it in a public forum. At the same time, he might choose to remain anonymous simply out of fear that harm may come to himself or his family. Therefore, although anonymity might be used to elude responsibility, it also shields one from public reproach.

C. Anonymity and Democracy

Because anonymity is an important component of free speech and privacy generally, the debate about anonymity on the Internet is, to some degree, a debate about the political and social freedoms in a democratic society.[92] Anonymity is a necessary component in people's ability to form ideas outside the watchful eye of their neighbors. Persistent and pervasive monitoring, or the perception of such monitoring, stifles exploration of activities or ideas that are out of the mainstream.[93] "Examination chills experimentation with the unorthodox, the unpopular, and the merely unfinished."[94] Radical ideas, minority religions, unconventional activity, and maybe even risky entrepreneurship will suffer if anonymity is eliminated. Lack of anonymity threatens people's ability to challenge authority or the dominant paradigm.[95] Minority vision and diverse thinking are the fuel that drives the engine of a pluralist society. The expansive democratic marketplace of ideas will be reduced to a corner store if people are not allowed to freely try all the products and contribute new ones.

American democracy is based on knowledgeable and reasoned self-governance. A representative government of federalism, checks and balances, and enumerated powers is based on distributed decision making by the citizenry. People must have robust and varied debate on issues of public policy in order to sustain such a system. Anonymity is a necessary component in allowing this robust debate to occur.

Some argue, however, that anonymity can be harmful in a democratic society.[96] If an idea is not attributed, a person cannot consider the source. There is a difference between the President of the United States making a statement and a patron at the local bar uttering the same words. Society credits statements based on their source. A system of attribution encourages thoughtful discussion and acts as a filter for sorting through the marketplace of ideas.

In balancing such arguments with the free speech principles of the First

---

[92] *See* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 500-01 (1995) ("In democratic society, information standards reflect specific conceptions of governance. . . . For private interactions and the relationship between citizens, both law and practice set the balance between dignity and free flows of information.").

[93] *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object,* 52 STAN. L. REV. 1373, 1427 (2000).

[94] *Id.* at 1426.

[95] Election by secret ballot is but one example of how anonymity is used to protect one's freedom to challenge established authorities in a democracy. *See McIntyre*, 514 U.S. at 343.

[96] *See, e.g.*, Branscomb, *supra* note 29, at 1642-43.

Amendment, the benefits of anonymity seem to far outweigh the negatives.[97] This article argues that in order to protect freedom of expression, diversity, pluralism, minority views, and democracy, we must allow for and protect anonymity.

D. Anonymity on the Internet

The ability to maintain anonymity on the Internet poses some unique challenges and questions not addressed in other situations. If everyone communicates anonymously in cyberspace, how do we achieve public policy goals, such as protecting minors from harmful content, preventing financial fraud, and preventing copyright infringement? Enforcement of such policies is based on the ability to identify and punish the perpetrator. These problems will only worsen as we expand the uses of the Internet. Certainly every "real-world" activity that we export to the Internet will have its own unique issues and challenges. Anonymity will only complicate these challenges. However, for the reasons discussed above, anonymity is an essential tool in protecting free speech and action on the Internet, even if accountability is marginally diminished.

E. Striking the Balance

Anonymity, like everything else, has a positive and a negative aspect. It is instructive to take each of these aspects to their logical conclusion. By advocating for the elimination of anonymity, one is establishing a platform for total social control.[98] Without anonymity, society could virtually eliminate all criminal and anti-social activity by monitoring and punishing citizens who step out of line. However, the elimination of crime through the elimination of anonymity would cost society its freedom. To the other extreme, society could engineer systems that force all actions to be taken anonymously. Total anonymity, however, would likely lead to serious inefficiencies in commerce and communications, as well as an erosion of one's sense of community with others.[99]

These absolutes are not our only choices. Society can allow for anonymity without forcing anonymity. We can embrace individual responsibility without accepting an omnipresent police state. In this middle ground, society allows individuals to choose anonymity within a system that holds them accountable for their actions.[100] The goal of this article is to describe a method to achieve a choice regime that allows for anonymity on the Internet.

IV. CONSTITUTIONAL, TORT, AND LEGISLATIVE APPROACHES: PRIVACY AS A

---

[97] While it might delay the process, we can give credence to ideas based solely on their content, without first filtering them by source.

[98] *See* LESSIG, *supra* note 27, at ix-xi (describing Vinge and Maddox's visions of a society that is monitored and controlled).

[99] *See infra* Part V-C (noting the inefficiencies involved in anonymous transactions).

[100] This conclusion does not solve the inherent conflict between anonymity and responsibility. Certainly, with a system of choice, those who want to undertake criminal activity will choose to remain anonymous and avoid accountability. However, this is a result we should be willing to accept given the alternative.

In *Code and Other Laws of Cyberspace*, Lawrence Lessig describes a process by which the original meaning and values of past constitutional decisions are preserved while adapting to novel technologies such as the Internet.[101] He calls this process "translation."[102] Lessig says that "different technologies are the different languages; and the aim is to find a reading of the Constitution that preserves its meaning from one world's technology to another."[103] Lessig explains that while courts have already made some core policy decisions, courts have yet to decide many others because of changing technology.[104] The challenge is to maintain the integrity of fundamental policy decisions, and the values behind those decisions, within the new medium.

Accepting Lessig's view, it is important to first evaluate how anonymity has been protected in the off-line world. This section has two distinct but overlapping goals: (1) to explore the different legal approaches to protecting anonymity and whether they will be effective in cyberspace; and (2) to identify the core values behind anonymity to be translated into cyberspace.

Currently, the right to conceal one's identity is a quasi-right.[105] It is protected within certain contexts and not in others. Privacy is not protected under any single legal doctrine. One only has a legal claim to privacy within constitutionally protected rights (i.e., speech, religion, and association), under tort law, or under specific statutory provisions. The right to anonymity is complicated and chameleon-like, changing with the surrounding circumstances.

A. The Constitutional Approach

The Constitution provides a number of tools to guarantee privacy. The Supreme Court has recognized First, Fourth, and Fifth Amendment privacy arguments.[106] While some of these constitutional arguments can be

---

[101] *See* LESSIG, *supra* note 27, at 119 (discussing the application of constitutional principles to modern technologies).

[102] *See id.* at 109.

[103] *Id.* at 119.

[104] *See id.* at 119-20 (discussing the Supreme Court's 1990 decision in Maryland v. Craig, 497 U.S. 836 (1990)).

[105] *See*, *e.g.*, Privacy Act of 1974, 5 U.S.C. §552a (1994 & Supp. V 2000); Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (1994 & Supp. IV 1999); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (1994); Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 (1994); Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2703 (1994); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) (protecting under the first amendment anonymous literary endeavors and political speech); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 466 (1958) (upholding right of NAACP members to associate free from state scrutiny of NAACP member lists).

[106] *See* Stanley v. Georgia, 394 U.S. 557, 564-65 (1969) (holding that mere possession of obscene material is protected by the First Amendment's implied right of privacy); Katz v. United States, 389 U.S. 347, 350 (1967) (holding that government eavesdropping violates privacy and is a "search and seizure" within the meaning of the Fourth Amendment); Boyd v. United States, 116 U.S. 616, 634-35 (1886) (holding that compulsory production of private papers in a criminal prosecution violates the Fourth and Fifth Amendments).

compelling, there is an overarching problem with all such approaches. The Constitution only limits government action against citizens; thus constitutional arguments cannot help the online actor whose privacy is violated by a private company.[107] Indeed, while the First and Fifth Amendment decisions illustrate judicial concern over government-compelled disclosure of identity, AOL compels almost thirty million people to disclose their identity every time they log on.[108] This is just one reason why constitutional arguments effectively address only half the problem.

Constitutional arguments do not directly constrain private actors and therefore do little to ensure anonymity. The Court, however, expounds on fundamental values in these decisions, highlighting another aspect of translation. These values arguably represent the collective view of our constitutional and democratic processes. These decisions carry weight beyond their direct application. Often, private actors take guidance from such decisions in creating private policy. For example, many private employers support their employees' right to free speech. Is this because the law mandates them to do so? No. It is because most employees assume and desire a respect for the values of free speech, not only from the government but from all institutions. Therefore, by looking at constitutional decisions, one gains an understanding of the values behind anonymity, which should be translated and used as a touchstone when creating private information systems.

B. Constitutional Cases and Claims

In a number of instances the Supreme Court has expounded the virtues of a constitutional right to privacy and anonymity. In *Griswold v. Connecticut*, Justice Douglas reasoned that because of a constitutional right to privacy, a state could not forbid the use birth control devices.[109] The *Griswold* Court found this right in the "penumbras" emanating from the First Amendment's right of association, the Third Amendment's prohibition against the quartering of soldiers in time of peace, the Fourth Amendment's right of the people to be free from unreasonable search and seizures, the Fifth Amendment's right against self-incrimination, and the Ninth Amendment's reservation of rights to the people.[110] Additionally, in *Roe v. Wade*, the Court recognized a fundamental right to privacy under the Fourteenth Amendment.[111]

While the *Griswold* and *Roe* privacy rights seem abstract and indirectly

---

[107] One commentator has noted another problem with the Constitutional approach to privacy. Robert Ellis Smith argues that the future of constitutional privacy seems limited to family and contraception under the current composition of the Supreme Court. *See* ROBERT ELLIS SMITH, THE LAW OF PRIVACY EXPLAINED § 1.18, at 41 (1993). Smith acknowledges, however, that the Court may be moving toward a new, potentially more expansive, conception of constitutional privacy. *See id.* § 1.19, at 43.

[108] *See* McVeigh v. Cohen, 983 F. Supp. 215, 217, 222 (D.D.C. 1998) (enjoining United States Navy from taking adverse action against plaintiff, whom the Navy had sought to discharge after AOL disclosed his identity in connection with a username that suggested he was homosexual); *supra* note 42.

[109] 381 U.S. 479, 485 (1965).

[110] *See id.* at 484.

[111] 410 U.S. 113, 153 (1973).

related to one's ability to remain anonymous, the First Amendment's guarantees of free speech and freedom of assembly have provided protections for anonymous speech and secret association.[112] In 1958, the Supreme Court held that the First Amendment protects a right of anonymous association and that a state therefore lacked the power to compel a local chapter of the NAACP to disclose the names of its members.[113] More recently, in the seminal *McIntyre* case, the Supreme Court held that the right to speak anonymously about political ideas is protected by the Constitution.[114] The Court determined that because anonymity is a component of the speech itself, a state could not compel disclosure absent strong justification.[115] In 1997, a federal district court applied the same logic to protect anonymity in online speech.[116]

The First Amendment provides other theories under which online privacy can be protected. Under the "compelled speech doctrine," courts have held that forcing speech violates the First Amendment.[117] The Supreme Court has ruled that there is no constitutional difference between compelled speech and compelled silence.[118] "[T]he First Amendment guarantees 'freedom of speech,' a term necessarily comprising the decision of both what to say and what *not* to say."[119] In *Riley v. National Federation of the Blind*, the Court stated that any statute mandating speech "necessarily alters the content of speech."[120] If the government cannot compel speech, it is questionable whether it can compel identification in online transactions.[121]

The First Amendment also may be used to provide a constitutional argument that one should be able to read anonymously.[122] The basis of this argument is

---

[112] *See*, *e.g.*, McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995); NAACP v. Alabama *ex rel*. Patterson, 357 U.S. 449 (1958).

[113] *See Patterson*, 357 U.S. at 462.

[114] *See McIntyre*, 514 U.S. at 342.

[115] *See id*.

[116] *See* ACLU v. Miller, 997 F. Supp. 1228, 1230, 1232 (N.D. Ga. 1997) (enjoining enforcement of a state law forbidding the false identification of a sender of electronic information).

[117] The Supreme Court has struck down laws that require citizens to disclose certain facts connected with other protected activities. *See*, *e.g.*, Riley v. National Fed'n of Blind, 487 U.S. 781, 795-97 (1988) (striking down statute that required professional fundraisers to disclose to potential donors the percentage of charitable contributions collected that was actually turned over to charity); Brown v. Socialist Workers '74 Campaign Comm., 459 U.S. 87, 98 (1982) (striking down law requiring political candidates to disclose names of campaign contributors); Buckley v. Valeo, 424 U.S. 1, 58-59 (1976) (per curiam) (invalidating law placing ceiling on campaign expenditures).

[118] *See Riley*, 487 U.S. at 797.

[119] *Id.* at 796-97.

[120] *Id.* at 795. The Court evaluated the statute under the stringent test for "content-based regulation of speech." *Id.*

[121] *Cf.* David W. Ogden, *Is There a First Amendment "Right to Remain Silent"?: The Supreme Court's "Compelled Speech" Doctrine*, 40 FED. B. NEWS & J. 368, 369 (1993) (questioning whether the compelled speech doctrine forbids the government from mandating that citizens provide specified information like income and other personal information on tax returns).

[122] *See* Cohen, *supra* note 84, at 1007.

that the uninhibited intake of information is part and parcel with its later expression, and should be protected as such.[123] The precedent for this argument originated in the Supreme Court opinions *Lamount v. Postmaster General*[124] and *Stanley v. Georgia*,[125] both of which dealt with one's ability to read without state interference or oversight. In *Stanley*, the Court said that one has "the right to be free from state inquiry into the contents of [one's] library."[126] Taken in conjunction with *McIntyre*, these cases present a compelling argument that the government should not monitor or interfere with one's online reading. Reading information from a Web page is an interactive process; the reader controls the presentation and content of the information. This makes online reading much more expressive in nature and closer to speech than reading hard copy materials. The First Amendment may cover this "expressive reading," thus encompassing a claim to anonymity.

In each instance above, the Constitution provides a limited privacy right if the actor is within certain parameters and is being limited by the government. Directly translating or applying these constitutional protections in cyberspace is possible, but not very helpful, due to the private actor problem.[127] These cases demonstrate, however, that privacy and anonymity are of constitutional importance and should be treated as such. The core values in these cases are the right to be left alone, the right to free expression, and the right to hide one's identity. These values are also reflected in common law privacy torts, which we may conceive as gap fillers in the constitutional privacy framework.

C. Common Law Privacy Torts

Traditional tort law protection of privacy is based on four theories: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) misappropriation of name or likeness for commercial purposes; and (4) publicity that places another in a false light.[128] While each of these theories might directly translate to protect invasions of online privacy, their application is limited.[129] As to the first three torts, no legal claim will succeed if the

---

[123] *See id.* (noting that the First Amendment should protect "the entire series of intellectual transactions through which [people form] the opinions they ultimately [choose] to express").

[124] 381 U.S. 301, 307 (1965) (striking down law authorizing interception of communist propaganda).

[125] 394 U.S. 557, 565 (1969) (striking down law that forbade the possession of "obscene" reading materials).

[126] *Id*.

[127] *See supra* note 107 and accompanying text.

[128] *See* RESTATEMENT (SECOND) OF TORTS §§ 652B, 652D, 652C, 652E (1977). These categories are not mutually exclusive, and like other common law, are not recognized by certain states.

[129] Some scholars, notably Richard Epstein, believe that privacy torts will develop to protect many online privacy violations. *See* Richard A. Epstein, *Privacy, Publication, and the First Amendment: The Dangers of First Amendment Exceptionalism*, 52 STAN. L. REV. 1003, 1006 (2000) (arguing that the First Amendment does not constrain the evolution of common law privacy torts in cyberspace).

complainant is aware of or can foresee data collection.[130] Additionally, any disclosure of information must be "highly offensive" to the reasonable person, a standard that places a high burden on plaintiffs.[131] Even more troubling, from the perspective of Internet privacy, is the fact that tort law varies significantly from state to state, with some states recognizing all such torts and others recognizing none.[132]

The intrusion upon seclusion theory imposes liability on "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns. . . ."[133] For this tort to apply, the invasion must be highly offensive to the reasonable person, although it is irrelevant whether or not the intruder discloses the information he obtains.[134] An Illinois appeals court found that American Express did not violate this tort when it collected and sold information that customers "voluntarily" gave.[135] It is clear that if a person is aware of or can foresee data gathering, a court will deem his or her disclosure of such information voluntary, and a complaint for the intrusion upon seclusion tort will not lie.

Giving credence to the *Restatement*, intrusion upon seclusion, by its terms, may be applicable in actions brought against invasions of privacy and anonymity online.[136] Many Internet identification technologies, such as cookies, intentionally intrude upon the solitude or seclusion of another. Despite this fact, the author is unaware of any plaintiff asserting such a claim. One reason could be that *Dwyer v. American Express Co.* and other similar cases have established a high hurdle as to voluntariness.[137] For example, many Internet users are aware of cookies, and most modern browsers can be set to reject them.[138] Therefore, a court may reject a complainant's privacy claim where the complainant voluntarily allowed cookies onto his or her system. However, as identification technology on the Internet proliferates, there will be more instances in which information is disclosed without this element of choice. For example, if IPv6 were implemented in its current form, a user's identity would be disclosed without the user having the option to conceal it.[139]

The second tort applies when a reasonable person would find the public

---

[130] *See* RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (requiring matter to be closed from public view).

[131] *See id.* § 652B.

[132] *See* 1 J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY §§ 6.1-.127 (2d ed. 1996) (discussing the states' adoption of some or all privacy torts).

[133] RESTATEMENT (SECOND) OF TORTS § 652B.

[134] *See id.* § 652B cmt. a, b.

[135] *See* Dwyer v. American Express Co., 652 N.E.2d 1351, 1354 (Ill. App. Ct. 1995).

[136] *See* Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L.J. 1089, 1106 (1998) (discussing how intrusion upon seclusion could be actionable without regard to physical intrusion and citing sources and rationales for protecting nonconsensual electronic intrusions into one's home).

[137] *See Dwyer*, 652 N.E.2d at 1354 (establishing involuntary obtainment of information as an element of intrusion upon seclusion).

[138] *See* Kang, *supra* note 29, at 1229-30 n.152 (noting that modern browsers "allow[] one to set preferences to accept all cookies, reject all cookies, or accept only cookies that return the originating server and warn the individual whenever cookies are set").

[139] *See supra* notes 66-74 and accompanying text.

disclosure of private facts to be highly offensive.[140] A district court recently relied on this tort to preliminarily enjoin the release of a videotape depicting Bret Michaels having sex with Pamela Anderson Lee.[141] The court found that Michaels was likely to overcome a presumption against public figures and succeed at showing that such a release would be highly offensive.[142] An argument could be made that online profiling, which creates a detailed description of one's personal characteristics, is actionable under this tort. However, it is not likely that even the most detailed profile would rise to the level of a "highly offensive" disclosure of a private fact.

The third privacy tort, the tort of misappropriation, must be an appropriation of one's name or likeness for another's use or benefit.[143] This tort most easily protects famous individuals from others who seek to free ride on their names or pictures. However, the *Restatement* covers other situations in which the tort may apply, including using a person's photograph without consent in an advertisement, impersonating another to gain information about a spouse, and filing a lawsuit in the name of another without the other's consent.[144] A complainant may apply this tort to a cyberspace claim arguing that detailed profile information is a likeness that others should not appropriate. At least three plaintiffs have unsuccessfully attempted to use the appropriation tort on such an information privacy theory to enjoin the sale of names and addresses to direct marketers.[145] Although none of plaintiff's cases were successful, the court's rationale in each case is now in question, potentially opening the door for future successful claims.[146]

The final privacy tort applies when one publicizes another in a false light that is both highly offensive to the reasonable person and done with knowing or reckless disregard as to the falsity of the portrayal.[147] An example of this

---

[140] *See* RESTATEMENT (SECOND) OF TORTS § 652D (1977).

[141] *See* Michaels v. Internet Entertainment Grp., Inc., 5 F. Supp. 2d 823, 828, 839-40 (C.D. Cal. 1998).

[142] *See id.* at 838 (balancing the right of publicity against matters of public interest).

[143] *See* RESTATEMENT (SECOND) OF TORTS § 652C.

[144] *See id.* § 652C cmt. b, illus. 1, 4, 6; *see also* Dwyer v. American Express Co., 652 N.E.2d 1351, 1355-56 (Ill. App. Ct. 1995) (citing RESTATEMENT (SECOND) OF TORTS § 652C cmt. b (1965)); William J. Fenrich, Note, *Common Law Protection of Individuals' Rights in Personal Information*, 65 FORDHAM L. REV. 951, 998-99 (1996) (noting that misappropriation applies to non-celebrities).

[145] *See* Fenrich, *supra* note 144, at 989-94 (discussing Avrahami v. U.S. News & World Rep., Inc., No. 96-203, (Cir. Ct. Arlington County June 13, 1996); Dwyer v. American Express Co., 652 N.E.2d 1351 (Ill. App. Ct. 1995); Shibley v. Time, Inc., 341 N.E.2d 337 (Ohio Ct. App. 1975)).

[146] *See id.* at 990-91, 993 (critiquing the court's rationale in *Shibley* and arguing that *Dwyer* was decided on the erroneous premise that there is no value in a single name and that value exists only in the compilation of individual names). One can now question the *Shibley* and *Dwyer* rationales given that some computer companies (including Free-Pc.Com) recently gave away computers and Internet access to people willing to disclose personal information. *See, e.g.*, Saul Hansell, *No More Giveaway Computers*, N.Y. TIMES, Nov. 30, 1999, at C1; Tom Spring, *Free PCs, But Not a Free Lunch*, CNN.COM, Feb. 10, 1999, *available at* <http://www.cnn.com/TECH/computing/9902/10/freepc.idg/index.html>.

[147] *See* RESTATEMENT (SECOND) OF TORTS § 652E. This tort is similar to, but not

tort occurs where a newspaper publishes a spurious inferior poem by an amateur writer signed with Robert Frost's name.[148] In the context of cyberspace, this tort might establish a claim against an online profiler who recklessly publicizes false information about a user.[149]

Privacy torts provide limited direct protection of anonymity in cyberspace. Plaintiffs must meet high burdens, including showing that data collection was unknown and not foreseeable and that the information disclosure was "highly offensive." Additionally, tort law does not provide universal protection as it varies significantly from state to state. Privacy torts do have an advantage over constitutional claims because they apply to both private actors and the government. However, this is little consolation for plaintiffs attempting to use these torts to vindicate perceived online privacy violations.

Even if these privacy torts cannot be directly applied in Internet cases, a detailed discussion of them helps identify the core values society seeks to protect, thus allowing us to translate those values in online privacy protection. The theoretical underpinnings of these torts are slightly different from, but arise out of, constitutional privacy values. The values behind these torts express that individuals have rights in personal information and that individuals deserve some degree of privacy based on a respect for individual dignity and autonomy.

D. Statutes

In order to protect anonymity, Congress has enacted a litany of specific legislation in areas not adequately covered by constitutional protections or privacy torts. However, these statutes only protect privacy within limited confines. For example, these statutes prohibit cable operators, videotape service providers, and government agencies from disclosing an individual's personally identifying information.[150] Additionally, because of rapidly

---

equivalent to, defamation. *See id.* § 652E cmt. b.

[148] *See id.* § 652E cmt. b, illus. 3.

[149] Like other privacy torts, the application of false light to online profilers is highly questionable because the disclosure must be "highly offensive" and known or reasonably known to be false. *See id.* § 652E.

[150] *See generally* MARC ROTENBERG, THE PRIVACY LAW SOURCEBOOK: UNITED STATES LAW, INTERNATIONAL LAW, AND RECENT DEVELOPMENTS 1-155 (1998). The Privacy Act of 1974 limits the disclosure of personal information by governmental agencies. *See* 5 U.S.C. § 552a (1994 & Supp. V 2000). The Cable Communications Policy Act of 1984 prohibits the disclosure of personally identifiable information by cable operators absent consent or a court order. *See* 47 U.S.C. § 551 (1994 & Supp. IV 1999). The Video Privacy Protection Act of 1988 limits the disclosure of personally identifiable information by videotape service providers. *See* 18 U.S.C. § 2710 (1994). The Driver's Privacy Protection Act of 1994 limits the release of personal information contained in one's motor vehicle record. *See* 18 U.S.C. § 2721 (1994). The Electronic Communications Privacy Act of 1986 restricts a provider of electronic communication or remote computing services from disclosing a subscriber's personally identifiable information to a government official. *See* 18 U.S.C. § 2703 (1994). Just last year, Congress introduced several bills aimed at protecting Internet privacy. The Consumer Internet Privacy Protection Act of 1999 would regulate the use and disclosure of subscriber information by ISPs. *See* H.R. 313, 106th Cong. § 2 (1999). The Social Security On-line Privacy Protection Act would limit an ISP's ability to reveal an

changing technology, these statutes are often ineffective at addressing Internet privacy issues. For example, when Congress first introduced the Consumer Internet Privacy Protection Act, Internet technology was such that an individual's TCP/IP address could only be tracked back to the ISP.[151] Accordingly, unless one disclosed his or her identity directly to a web site, the web site provider had to request the user's personal information from the ISP. If Congress had drafted the Consumer Internet Privacy Protection Act to prohibit ISPs from disclosing such information, this statute would have protected online anonymity. In any case, such legislation could now be superfluous given PSNs and the proposed IPv6 standard.[152] Both of these technologies allow Web sites to identify specific users, down to the desktop level, regardless of disclosure restrictions Congress places on ISPs.

While these privacy statutes have only limited direct applicability in supporting anonymity over the Internet, they are relevant to this discussion. Even more than constitutional decisions, these statutes represent Americans' collective support for the values embodied in privacy and anonymity. These are values that must be translated on the Internet.

E. Legal Protections Summary

Because there is no absolute right to privacy,[153] constitutional claims, privacy torts, and federal statutes have created a patchwork of protection that protects privacy only within certain limited situations. These approaches have considerable weaknesses when applied to privacy on the Internet. Constitutional claims do not address the most prevalent source of privacy violations—private companies. Privacy torts are sporadically available and only enforceable through private litigation.[154] Federal statutes, due to rapidly changing technology, are inflexible and often cannot address the core problems related to Internet privacy. An alternative solution is needed.

V. ACHIEVING TRANSLATION THROUGH PETS

We can achieve translation of the anonymity values that underlie the constitutional, common law, and legislative approaches to privacy through numerous methods. First, Congress could pass new laws that directly and clearly give a person the right to remain anonymous while on the Internet. Second, courts could apply existing privacy torts more vigorously to online violators. Third, to induce companies to act in a pro-privacy manner, Congress

---

individual's Social Security number or related personal data. *See* H.R. 91, 107th Cong. § 2 (2001). The Freedom and Privacy Restoration Act of 1999 would also limit the use of Social Security numbers, and would prohibit creation of government identification cards. *See* H.R. 220, 106th Cong. § 2 (1999). All of these bills have been referred to committee. *See EPIC Bill Track*, PRIVACY INFO. CTR., Mar. 27, 2001 (tracking numerous online privacy bills), *available at* <http://www.epic.org/privacy/bill_track.html>.

[151] Remember that generally, ISPs assign a temporary TCP/IP address to their dialup customers. *See supra* notes 39-41 and accompanying text.

[152] *See supra* Part II.

[153] *See supra* note 2.

[154] *See* Neal T. Buethe, *Things to Come in Minnesota: Ways in Which the Privacy Tort Has Affected Employment Law in Other States*, 23 HAMLINE L. REV. 38, 41 (1999).

could threaten regulation. Fourth, we could establish watchdog groups that would police online actors for privacy violations. However, all such methods (some of which are currently being attempted) have limited effectiveness. If we rely on these methods, some people will always "get around" the rule or simply refuse to comply.

This paper advocates a more direct and dynamic approach. We should approach the translation of anonymity on the Internet through "code" by developing and implementing privacy-enhancing technologies (PETs).[155] PETs can achieve anonymity on the Internet through software and hardware that shields us from technological identification. By developing and implementing PETs, we can protect privacy and combat identification technology in the ongoing technological arms race.

While this answer may seem crude and unsatisfying to highbrow legal scholars (many of whom would rather derive a creative legal theory to apply existing law or craft legislation that gives people a statutory right to remain anonymous), PETs are an effective solution to achieving anonymity on the Internet. As such, PETs must be supported by policy and recognized as more than just self-help. Achieving translation of privacy values in cyberspace requires us to uphold the core values behind offline constitutional, common law, and legislative solutions to privacy. PETs effectively accomplish just that.

A. Choosing Between Formal and Material Conditions to Protect Anonymity

We can protect privacy through either formal or material conditions.[156] Formal conditions are rules or norms.[157] Such rules can be legal, moral, customary, or some combination thereof.[158] Formal conditions include laws against spying and "conventions of modesty or reserve, [and] of appropriate levels of curiosity or prying."[159] Material conditions of privacy include physical realities that prevent others from gathering information about another.[160] Material conditions include fences, locks, tinted windows, clothing, distance, and isolation.[161] PETs are a type of material condition.

While formal conditions of privacy can be effective without material conditions being in place,[162] material conditions more reliably prevent invasions of privacy.[163] Material conditions do not rely on an individual's sensibilities or level of respect for the law.[164] Material conditions have a

---

[155] Derived from Lessig's work, "code" in this context means any combination of software and hardware or any technological solution. *See* LESSIG, *supra* note 27, at 6.

[156] *See* Reiman, *supra* note 11, at 43.

[157] *See id.*

[158] *See id.*

[159] *Id.*

[160] *See id.*

[161] *See id.*

[162] *See id.* ("[P]eople packed like sardines in a rush-hour subway train have a way of respecting each other's privacy even though they have, materially, extensive access to one another's bodies.").

[163] *See id.*

[164] *See id.*

firmness and certainty that formal conditions cannot achieve.[165] Material conditions empower a person to act because he knows his privacy is protected.[166] This is illustrated in the security one feels from having a lock on his door, as opposed to relying on the law, to prevent his house from being robbed.

As related to anonymity on the Internet, material conditions are superior to formal conditions because formal conditions do little to alleviate the control of the Cyber-Panopticon. If there are rules against monitoring, but monitoring technology is available, the chilling effect remains, although maybe to a lesser degree. For example, imagine that you want to run outside your house naked but you do not want anyone to see you. You certainly would not do this at 2:00 p.m. on a Saturday when everyone is at home. Now imagine it is 3:00 a.m. on a Tuesday morning. Would you run outside now? You may be more likely to do so because you know that most people are sleeping and your chances of being seen are relatively low. However, you might still have some reservations—not because you believe anyone *will* see you, but because of the possibility that someone *may* see you.

The fear associated with running outside at 2:00 p.m. on a Saturday, when everyone is at home, is like an Internet without any privacy protection. Running outside at 3:00 a.m. on a Tuesday is like an Internet with formal rules against monitoring—while the chance of monitoring is decreased, the possibility is still there. Now imagine that you want to run outside your house naked, but before you do, you want to become invisible. If this material condition (the ability to turn invisible) can be achieved, it would not matter whether people were at home and awake, because you cannot be seen. Formal rules become irrelevant when material conditions provide a solution.

Another reason why material conditions are superior to formal conditions is because formal conditions have limited value where the goal is uninhibited freedom of expression. If one perceives that he is being monitored, his behavior will be constrained whether or not he is actually being monitored.[167] This constraint is present even when one does not believe he is being monitored, but knows it is a possibility.[168] As indicated in Part II, the Panopticon is effective even if no one is in the guard tower.

A further reason why material conditions are superior to formal conditions is because American laws, rules, and customs are limited and ineffective at covering the entire worldwide Internet. Presumably we could overcome this problem by enacting international formal conditions (i.e., treaties and other international agreements). However, this is a daunting task to say the least. The worldwide, distributed nature of the Internet poses a substantial, perhaps insurmountable, obstacle in the path of effective formal conditions. In contrast, we can successfully implement material conditions such as PETs without global coordination.

---

[165] *See id.*

[166] Formal conditions of privacy cannot fully guarantee privacy against material conditions for invading privacy. *See id.* at 43-44.

[167] Like the Panopticon metaphor, the experience and perception of our visibility constitutes a threat of social control and impaired liberty. *See id.* at 28, 43-44.

[168] *See id.*

B. Application of Currently Available PETs

PETs can be used to counteract technical identifiers like TCP/IP addresses, domain names, cookies, and PSNs. Anonymizer Incorporated offers a service that employs such PETs.[169] Anonymizer surfing, or proxy surfing, allows one to use the Anonymizer server as a "proxy," or gateway, to the rest of the Internet.[170] By proxy surfing, the end user makes only the Anonymizer TCP/IP address available to other web pages.[171] This effectively hides the TCP/IP address of the end user.

Another PET, the anonymous remailer, hides domain names or other identifying information that is attached to emails. Remailers strip the sender's user name and address from an incoming email and replace this data with a dummy address (for example, johnsmith@aol.com becomes az3234@remailer.com).[172] Remailers also strip away all email headers, which identify the route the email took in reaching the remailer.[173] The email message is forwarded to the sender's desired destination without any information that might link the message to the original sender.[174]

Numerous PETs address anonymity concerns associated with the placement and access of cookies. First, the easiest option is for end users to set their Web browsers to reject all incoming cookies.[175] Second, software companies like Network Associates and Zero-Knowledge make products that warn end users about cookies, encrypt cookie files, and prevent cookies from being set or accessed.[176] Third, by proxy surfing through a company like Anonymizer, one can prevent cookies from being transmitted or accepted.[177] However, it should be noted that these anti-cookie methods defeat the benefits cookies provide, such as permitting a Web site to customize information to a particular end user.[178]

---

[169] *See supra* note 44.

[170] *See Go Deep Undercover*, PC/COMPUTING, Nov. 1998, at 154, 154 (discussing various PETs, including proxy surfing).

[171] *See id.*

[172] For an extended explanation of remailers, *see* André Bacard, *Anonymous Remailer FAQ*, Feb. 2, 2001, *available at* <http://www.andrebacard.com/remail.html>.

[173] *See id.*

[174] *See id.* Forwarding the message to other remailers, thus "linking" remailers together such that no one remailer has the link back to the originator's email address, can enhance remailer privacy.

[175] Users can set most modern browsers to reject all incoming cookies. *See* Kang, *supra* note 29, at 1229-30 n.152.

[176] *See* Agam Shah , *McAfee Ships Cookie-Cleaning Software*, NETWORK WORLD, Sept. 25, 2000 (discussing Network Associates' Quick Clean, software that assists users in deleting cookie files), *available in* LEXIS, News Library, Nww File; *Zero-Knowledge Systems Unveils Free, Easy-to-Use Software that Protects Consumer Privacy on the Internet*, BUS. WIRE, Dec. 13, 2000 (discussing software that includes Cookie Manager, a utility that lets users decide which cookies to keep and which to block or delete), *available in* LEXIS, News Library, Bwire File.

[177] *See What Anonymous Surfing Does to Protect You*, ANONYMIZER.COM, *available at* <http://www.anonymizer.com/services/paidSurf.shtml>.

[178] *See* Kang, *supra* note 29, at 1227.

There is also a technological solution to the PSN identification system.[179] Due primarily to pressure from privacy groups, Intel has released a piece of software that, upon computer boot-up, will allow a user to suppress the PSN that is embedded in the computer's microchip.[180] While this software is not foolproof,[181] it can be an effective means to prevent another computer from accessing the PSN, thus preventing individual user identification.

Although IPv6 is not yet implemented, there will likely be PETs that can address its identification features as well. One solution might be similar to current proxy surfing where a person uses another machine to mask his TCP/IP address. A derivation of such proxy surfing that might be effective with IPv6 is called Network Address Translation or NAT. Currently, firewalls and proxy servers use NAT to allow multiple people within an organization to communicate on the Internet through one TCP/IP address.[182] Organizations, or even ISPs, could use a similar method to limit the use of identifying information in IPv6.

C. Costs and Limitations of PETs

Remailers, NAT, proxy surfing, cookie management, and PSN suppression software are potential solutions to the online anonymity problem. These solutions, however, are not perfect or without cost. First, by using remailers or proxy surfing, the end user is relying on the idea that the middleman will not disclose the end user's true identity.[183] Some of these services may actually have nefarious intent and others may be "sting operations" run by law enforcement officials.[184] In addition, anonymity services provide that they can disclose a customer's identity under operation of law or if the user violates the service agreement.[185]

Second, anonymity services and software often come at a price. Indeed,

---

[179] Another material condition could eliminate the threat of the PSN. A user could choose a microprocessor that does not have the PSN, such as an AMD chip or a non-PIII Intel chip.

[180] *See* Declan McCullagh, *Intel Nixes Chip-Tracking ID*, WIRED NEWS, Apr. 27, 2000, *available at* <http://www.wired.com/news/politics/0,1283,35950,00.html>.

[181] *See Pentium III Processor Serial Number Exploit Page*, ZEROKNOWLEDGE, *available at* <http://www.zeroknowledge.com/p3/home.asp>.

[182] Network address translation, or NAT, works by having a firewall act as an intermediary between the internal requesting machine and the external Internet server. The firewall logs the address of the originating machine, but sends out the request using its own TCP/IP address. When the Internet server responds the firewall forwards the results back to the internal machine. *See*, *e.g.*, *eTrust Internet Defense - Firewall FAQ's*, COMPUTER ASSOC., *available at* <http://www.computerassociates.com/solutions/enterprise/etrust/firewall/faq.htm>.

[183] *See* Bacard, *supra* note 172 (noting that with one type of remailer, "[y]our privacy is as good as the remailer operator's power and integrity to protect your records").

[184] *See id*. (raising the possibility that some remailers may be government sting operations).

[185] *See*, *e.g.*, *Anonymizer.com User Agreement 8.2*, ANONYMIZER.COM (explaining that a customer's identity can be disclosed for a number of reasons, including by operation of any law, or because the customer engaged in "spamming," a seemingly minor violation), *available at* <http://www.anonymizer.com/docs/legal/agreement.shtml>.

most providers charge annual or monthly fees for their products and services.[186] As a result of this cost, a number of people will be unable to purchase PETs, thus exposing themselves to identification technology.[187]

Third, there are indirect costs to the user of these products. These include: (1) slower web page access with proxy surfing; (2) a more complicated and lengthy sending and receiving process with remailers; (3) lack of access to sites that require cookies; (4) added software overhead for PSN suppression software; and (5) more complicated information systems with the implementation of NAT. Additionally, due to the changing nature of technology, even the makers of PETs admit that anonymity cannot be guaranteed by the use of such products or services.[188]

Fourth, the effectiveness of PETs is limited for users attempting to make purchases online. To complete a purchase over the Internet, the customer must learn about the product, pay money to the merchant, and take possession of the product. Normally, the user would accomplish this by accessing the site, paying with a credit card, and providing his or her shipping address. This process is by no means anonymous. Theoretically, PETs and other material conditions can allow this transaction to occur anonymously. For example, using the PETs described above, one can anonymously browse a site, pay with anonymous digital currency,[189] and have the product delivered to a pickup location or to a post office box that is held under an assumed name. However, such a process is currently burdensome because of the limited availability of digital currency and the expenses associated with traveling to a different location to pick up the product.

Finally, the greatest limitation of PETs lies in the fact that they are not widely available "standard" software and hardware.[190] Few users know about

---

[186] *See*, *e.g.*, *Sign Up for an Account*, ANONYMIZER.COM (providing anonymizing service packages at various prices), *available at* <http://www.anonymizer.com/signup/sign_up.shtml>.

[187] Direct costs represent one area in which formal conditions often have an advantage over material conditions. For example, it is cheaper to pass a law against robbery than to buy state of the art locks for every household.

[188] *See* Lance Cottrell, *Mixmaster & Remailer Attacks*, Mar. 3, 1998 ("Even if you are using a perfect network of remailers, you can still be tracked."), *available at* <http://www.obscura.com/~loki/remailer/remailer-essay.html>.

[189] Digital currency is a system in which cash-like electronic payments are made over the Internet. For example, imagine that A uses digital currency to buy an item from B. Under the digital currency model, A pays cash to Bank X. Bank X issues A a "token" or "coin," which is a computer file identified by a serial number that is chosen by A. This token is stored on A's computer until she sends it to B in exchange for the item. B can then convert the token back into cash at Bank X. Pursuant to a computer blinding process, the serial number designated by A remains unknown to the bank. Thus, when the bank redeems the token, it can verify its authenticity but cannot identify it with A. *See* Julia Alpert Gladstone, *Does The EC Council Directive No. 95/46/EC Mandate the Use of Anonymous Digital Currency?*, 22 FORDHAM INT'L L.J. 1907, 1911 (1999).

[190] It should be noted that Zero-Knowledge Systems' Freedom 2.0 Internet Privacy Suite is a leading all-in-one PET that addresses most of the concerns raised in this article surrounding Internet privacy including issues related to cookies, email, TCP/IP addresses, and others. However, to date, Freedom and other such products have not been widely

PETs and fewer still regularly use them. This problem needs to be addressed through policy and market reforms.

Despite these costs and limitations, PETs are the best solution to protect anonymity on the Internet. As indicated above, laws and other formal conditions have serious limitations. The greatest limitation is a reliance on others' sensibilities and level of respect for the law. PETs allow one to remain anonymous without having to rely on others. We can overcome the limitations and costs of PETs with supporting policies and developing markets. If universally implemented, PETs will overcome the chilling effect of identification technology and empower users to read, act, and communicate over the Internet without hesitation and with complete freedom.

D. Forces Against PETs and Anonymity

While protecting anonymity through PETs is desirable, the development and implementation of PETs is tied to economic market conditions. PETs are consumer products, which are subject to the whims of supply and demand. To be a desirable and viable solution, PETs must effectively translate the values of anonymity to cyberspace. If PETs are not widely available, why are there not more private companies developing PETs to meet consumer demand? Why is the technological trend moving so rapidly toward the Cyber-Panopticon, instead of toward anonymous Internet interaction? The answer lies in the political and market forces that shape our society.

The commercial value of the Internet and the massive public support for crime prevention drive the economy for identification technology. The next section examines these market forces to show a trend toward the Cyber-Panopticon, a trend that will continue in the absence of a proactive implementation of PETs.[191]

1. Weak Market for Privacy in the New Economy

Opposing the rapid development and implementation of identification technology are those people in the market who are involved with PETs. People who want to remain anonymous in their daily activities are developing, buying, and implementing such technology. However, some evidence suggests that beyond a relatively small privacy advocacy coalition, the broad market for privacy is only beginning to develop.[192] Why is that?

---

adopted in the market. Information about Freedom 2.0 can be found at <http://www.freedom.net>.

[191] While the next section focuses on market, social, and political forces, there are also practical reasons for the proliferation of identification systems. One such reason is a phenomenon called "function creep." This is a process in which agencies use systems for additional purposes that they did not announce or intend at the beginning of the plan. *See* David A. Petti, *An Argument for the Implementation of a Biometric Authentication System ("BAS")*, 80 J. PAT. & TRADEMARK OFF. SOC'Y 703, 726 (1998). For example, one's Social Security number was originally only to be used by employers. Later the government expanded its use to all federal employees and in 1961, the IRS used it to identify taxpayers. Today many private universities and organizations use the SSN as a method of universal identification. *See id.* at 727.

[192] The Electronic Privacy Information Center found in 1997 that only 17 of the top 100

First, the development of identification technology supports commerce in cyberspace and runs contrary to a robust privacy market. As described earlier, each step in a remote consumer transaction is time consuming and costly. Methods of identification technology, like the PSN, assist remote transactions by facilitating information transfer, thus reducing time and transaction costs.

Second, political and market forces in the new economy favor corporate actors over privacy advocates. In *All the President's Men*, Deep Throat advises Woodward and Bernstein to "follow the money."[193] This advice facilitated the uncovering of the Watergate scandal; it is also apt for providing insights into the incentives of policy makers and business people. In the last ten years, the "money" has been gravitating towards the Internet. Companies like Cisco, Microsoft, and AOL dominate news headlines as the world's most valuable companies. In March of 2000, Cisco ended a trading day with a "market capitalization of $579.2 billion, slightly ahead of Microsoft's $578.2 billion."[194] This market capitalization was close to Russia's estimated gross domestic product of $593.4 billion in 1998.[195] Electronic commerce companies like Amazon.com boast staggering market value even though they have yet to show a profit.[196] Many business leaders and politicians point to the Internet as the driving force behind much of the economy's recent growth.[197] This has created a political environment in which anything Internet related is "hands off" from a regulation perspective.[198] Indeed, the Internet is even supported through federal funds.[199] It is in this environment of enormous

---

Web sites reported by "www.100hot.com" had privacy policies and that few of these policies were easy to find. *See Surfer Beware: Personal Privacy and the Internet*, ELEC. PRIVACY INFO. CTR., June 1997, *available at* <http://www.epic.org/reports/surfer-beware.html>. Similarly, in a 1998 survey of 1,400 American Internet sites, the Federal Trade Commission "found that only 2% had posted a privacy policy in line with [policies] advocated by the commission . . . ." *The End of Privacy*, ECONOMIST, May 1, 1999, at 22, 23. By 2000, another FTC survey showed that although an increasing number of web sites posted privacy policies, only one in five of these posted policies offered meaningful privacy protection. *See Net Privacy Promises Again Come Up Short*, USA TODAY, May 23, 2000, at 28A.

[193] ALL THE PRESIDENT'S MEN (Warner Bros. 1976).

[194] *Cisco Closes as World's Most Valuable Company*, PLANET IT, Mar. 29, 2000, *available at* <http://www.planetit.com/techcenters/doc/advanced_ip_services/news/PIT20000329S0001>.

[195] *See Cisco Tops Microsoft as Most-Valued Company*, MUZI NEWS, Mar. 25, 2000, *available at* <http://news.muzi.com/ll/english/63755.shtml>.

[196] *See* Lee Barney, *E-tailing Beacon is Flickering*, ABC NEWS.COM, Dec. 21, 1999, *available at* <http://www.abcnews.go.com/sections/business/thestreet/amazon001220.html>.

[197] President Clinton's 2000 State of the Union speech addressed the economic force of the Internet. *See* President Bill Clinton's Address Before a Joint Session of Congress on the State of the Union Address (Jan. 27, 2000), *available at* <http://www.c-span.org/executive/stateofunion/sou00_trans.asp>.

[198] *See* WILLIAM J. CLINTON & ALBERT GORE, JR., A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE (1997), *available at* <http://www.iitf.nist.gov/elecomm/ecomm.html>.

[199] The "e-rate" program imposes a tax on long-distance service and directs those funds to schools and libraries for Internet connections. *See Myths Surrounding the E-Rate*, Dec. 8,

wealth creation and political support that companies and politicians have supported identification technology. Electronic commerce companies realize the economic benefit of identification technologies and have used their power to advance technological developments in this area.[200]

Third, from a theoretical perspective, the market theory for privacy is questionable at this stage in the Internet's technological development. In a rapidly growing technology market, a number of other factors overshadow the privacy issue (e.g., price, quality of service, features, technical support, etc.). Later, when the market matures, the pro-privacy features or services will likely occupy a competitive niche.[201] However, in this growth stage of the Internet, the market for anonymity is either failing or nonexistent. ISPs are not proclaiming anonymity as a competitive advantage and it seems that few even have a privacy policy. In its dial-up service user agreement, one major ISP, PSINet, states, "given the current regulatory and technical environment [users] should not have an expectation of privacy in . . . online activities."[202] Such ambivalence from major Internet companies confirms that market forces are not encouraging anonymity on a large scale.[203]

Finally, efficient markets for any product or service depend on wide distribution of information. In the market for privacy, there are significant incentives for users of identification technology to suppress information about identification technologies and available PETs. For example, law enforcement authorities and surveillance companies do not want the general public to know the details of how sophisticated monitoring technologies work or the fact that they even exist.[204] Similarly, DoubleClick is not going to advertise the availability of cookie suppression software. Economic models advocate that for a capital market to operate at peak performance, all actors must have complete information.[205] While these optimal conditions can never completely exist, in this instance there are significant forces working against the distribution of information related to PETs.

1998, *available at* <http://www.house.gov/lofgren/e-myths.html>.

[200] As discussed above, technologies that identify users help Web-based merchants gain and store information about customers. This in turn enables faster, more efficient, and customized service.

[201] For example, consider the cordless telephone. When this technology was first developed, any telephone could easily be intercepted by means of a radio scanner. Later, companies developed encryption technology to prevent the interception of these telephone conversations. These telephones were more expensive and not widely available. Even today, such technology has not been widely accepted for home-based cordless telephones.

[202] *iPass Terms of Service*, PSINET, July 28, 2000, *available at* <http://www.psi.net/access/ipass/ipassagreement.html>.

[203] *See* Mark E. Budnitz, *Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate,* 49 S.C. L. REV. 847, 867 & n.130 (1998) ("'[W]e have not yet seen voluntary self-regulation work in the privacy arena.'") (citations omitted).

[204] *See* Jonathan I. Edelstein, Note, *Anonymity and International Law Enforcement in Cyberspace,* 7 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 231, 237 (1996) (alluding to the hindering effect Internet anonymity has on law enforcement efforts).

[205] *See* DAVID C. COLANDER, MIRCROECONOMICS 196 (1993).

2. Crime Prevention

In addition to a strong market for identification technology, public support for crime prevention has also helped drive the development of identification systems. In *Katz v. United States*, the government argued that the ability of government to wiretap and monitor telephone conversations was a necessary part of law enforcement.[206] To catch criminals, the government must be able to gain knowledge of illegal activities and to identify the perpetrators.[207] This same justification constitutes a major force behind the development of identification technologies.

The argument is intuitive. In order to deter crime, one must be able to catch criminals. In order to catch criminals, law enforcement authorities must be able to identify online actors. Therefore, enforcement authorities are expected to push for better monitoring technologies and work against technology that allows individuals to remain anonymous. As mentioned above, current Internet communication protocols do little to identify hackers or monitor Internet traffic. Therefore, when hackers attacked a number of major Internet sites in early 2000, law enforcement authorities had limited means with which to catch the criminals. The lack of tools has prompted law enforcement authorities to push for better identification mechanisms on the Internet.[208]

E. Strengthening the Market and Supporting PETs

Given the limitations of PETs and the forces working against their adoption, what can be done to support universal implementation of PETs? Government, privacy advocacy groups, and technology companies can do three things to accomplish this goal. Of course, the market for privacy is in its infancy and will become stronger as we approach the Cyber-Panopticon.[209] However, society needs to implement these recommendations in order to ensure that the values of anonymity are translated to the new medium of the Internet. The recommendations are as follows:

1. Educate the public as to the availability of, and the need for, PETs.
2. Encourage research and development of PETs though federal funds.
3. Encourage technical bodies, such as the IETF, to adopt technological standards that will support PETs.

As discussed above, the market for PETs is weak due to a strong countervailing market for identification technology and the relative lack of

---

[206] 389 U.S. 347, 355-56 (1967) (noting that wiretapping warrants fill "legitimate needs of law enforcement") (citations omitted).

[207] *See id.* (recognizing the "legitimate needs of law enforcement") (citations omitted).

[208] *See* Hamilton, *supra* note 36.

[209] There is some evidence to support that the market for privacy is becoming stronger. An increasing number of web sites are posting privacy statements, *see supra* note 192; Intel announced they would not continue to use the PSN feature, *see supra* note 62; and EarthLink, the nation's third largest ISP, has started an advertising campaign in which they tout customer privacy as an advantage of their service over other ISPs. *See Earthlink Debuts New Privacy-Focused Ad Campaign*, EARTHLINK.COM, Feb. 26, 2001, *available at* <http://www.earthlink.net/about/pr/privacy_ad_focus.html>.

information about PETs. Therefore, to create a more robust market for PETs, interested parties, including the federal government, should educate the public as to the availability of, and the need for, PETs.[210] By making a concerted effort to increase the information available about such products, the demand will increase.

The second recommendation is intended to increase the availability and quality of PETs. Identification technology is developing at a rapid rate and the PETs that are effective today will be outdated soon. PETs and identification systems will always compete in a technological arms race. The objective of this second recommendation is to tilt the playing field in favor of PETs. We need direct federal subsidization of research and development of PETs at colleges, universities, and private firms.

The final recommendation is aimed at ensuring the long-term and universal implementation of PETs. Along with hardware and software companies, technical standards bodies like the IETF control material conditions on the Internet. Given current and future Internet protocols and standards, we need to ensure that we can universally implement PETs.

It is uncertain how effective these recommendations will be at overcoming the forces against the adoption of PETs. However, these recommendations address some of the key problems with the current market, including lack of information and availability, lack of incentives to use and develop PETs, and lack of universal implementation.

Lessig and others might argue that the measures this paper recommends are too indirect to solve the problem. Lessig points out that law regulates markets and directly controls material conditions.[211] Lessig advocates the direct regulation of code, thus legislating material conditions by mandating that software and hardware companies include or not include certain features consistent with public policy goals.[212] In many ways, however, such direct regulation is overly intrusive and unnecessary given the developing market for PETs.[213]

The recommendations above are intended to help the development of PETs. The adoption of these recommendations would support the wide availability of PETs, thus making anonymity a choice for online users.[214] Such a choice would enable the translation of anonymity values to the Internet.

VI. CONCLUSION

On some level, there is no doubt that Americans value anonymity. However, Americans are unknowingly giving up anonymity in exchange for

---

[210] This could be accomplished through a variety of methods, including Internet and traditional media advertising campaigns and through educational programs in schools and universities.

[211] *See* Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661, 666 (1998).

[212] *See* LESSIG, *supra* note 27, at 51.

[213] The direct regulation approach would be more agreeable if there was evidence of insurmountable market failure for PETs.

[214] Certainly, it would not be wise to impose systems that compel anonymity on Internet users who wish to disclose their identity. Such disclosure might benefit a user by facilitating commerce or allowing the delivery of customized information.

convenience, higher productivity, faster communication, better crime prevention, and personalized information. Such advancements are facilitated by the rapid development of identification technologies. The proliferation of the Internet and these technologies is leading us toward a world in which our every action is monitored and stored, thus creating the Cyber-Panopticon. This technological trend toward persistent identification threatens a number of core values that society has traditionally protected, including freedom of expression.

In effort to protect anonymity and counteract anti-privacy technology, scholars, policy makers, and privacy groups have suggested a number of approaches, including constitutional arguments, common law privacy torts, and legislation. While none of these approaches have proven effective, they have unveiled several core values behind anonymity that deserve protection. Translation of these values can be achieved most effectively through a market that implements PETs.

While some PETs are currently available, the PET market is in its infancy and significant forces oppose its development. We should support the PETs market through three sets of actions: educating the public about PETs, subsidizing the research and development of PETs, and encouraging technical standards bodies to support PETs.

These recommendations are preferable to laws and other formal conditions. Formal conditions have serious limitations, including a reliance on other's sensibilities and level of respect for the law. The implementation of PETs, on the other hand, allows one to remain anonymous without relying on such extraneous factors. PETs have some limitations and come at a cost, but these problems can be overcome with supporting policies and markets. If universally implemented, PETs will overcome the chilling effect of identification technology and empower one to read, act, and communicate over

the Internet with freedom. On the other hand, if PETs are not adopted, the Internet will become a medium of persistent identification that undermines the basic privacy values that are important in a free society.