Journal of Law and Policy

Volume 5 | Issue 2 Article 7

1997

Computer Cookie Control: Transaction Generated Information and Privacy Regulation on the Internet

Joshua B. Sessler

COMPUTER COOKIE* CONTROL: TRANSACTION GENERATED INFORMATION AND PRIVACY REGULATION ON THE INTERNET

*Joshua B. Sessler***

It is important that we tackle these issues now before we travel down the information superhighway too far and realize perhaps we've made a wrong turn.[1]

INTRODUCTION

The ubiquitous use of computers by the government and private industry to store data pertaining to citizens and patrons has given rise to increasing concerns about privacy.[2] Although governmental use of such data is regulated, private industry has successfully resisted application of significant regulation.[3] Retail stores, credit bureaus and telecommunication companies have maintained virtually unhindered access to information about a customer's usage

---

* A "computer cookie" is a computer file that collects information about a computer's activity. Farham Memon, *Will Cookies Make the Cut?*, INTERACTIVE WK., Dec. 9, 1996, at 1.

** Brooklyn Law School Class of 1997. The author would like to thank Professor Michael Madow for his valuable suggestions during the formulation of this Note. A special thank you to Phyllis Belkin and Sofie Zoe Belkin-Sessler who were so understanding and supportive.

[1] 142 CONG. REC. E1145-01 (daily ed. June 20, 1996) (statement of Rep. Markey) [hereinafter Markey Statement].

[2] *See* HENRY H. PERRITT, JR., LAW AND THE INFORMATION SUPERHIGHWAY: PRIVACY, ACCESS, INTELLECTUAL PROPERTY, COMMERCE, LIABILITY § 3.1 (1996) (providing an overview of the privacy issue).

[3] Joel R. Reidenberg & Francoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in the Network*, 30 WAKE FOREST L. REV. 105, 113 (1995). *See infra* Part III.A-B (discussing privacy legislation's effect on government and the private sector).

and preferences, sometimes even without the customer's knowledge.[4] These entities often sell a consumer's personal information such as buying habits, credit records and telephone usage,[5] to direct marketing companies.[6]

Currently, on-line transactions over the Internet and other networks[7] offer analogous information to network service providers and system administrators.[8] In addition to data provided directly by the user, the electronic transmission itself leaves a "personal profile"[9] sometimes without the user's knowledge.[10] This "imprint" has been referred to as "transaction generated

---

[4] Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights,* 44 FED. COMM. L.J. 195, 202-03 (1992).

[5] *Id.* at 205-06.

[6] PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 228 (1995).

[7] The Internet is part of the global network of computers linked via telephone lines. *See* CHRISTOPHER CRUMLISH, THE INTERNET DICTIONARY 97 (1995). The World Wide Web ("Web") is a segment of this same network where special computer languages can be used to create "Web pages" of text and graphics that can be linked to other pages on the Web. *Id.* at 214 (describing a Web page as a "document on the World Wide Web, usually containing . . . links to other documents on the Web"). A "home page" is a starting page on the Web "with links to other related pages." *Id.* at 89-90. These can be thought of as an entryway or table of contents to an individual's or an organization's "Web-site"—a collection of pages. Each site is really a collection of computer files available for viewing, downloading (taking a copy) or interacting (sending comments or questions, or purchasing items). Home pages are "visited" by network users who either type the page's Web address or Uniform Resource Locator ("URL") into their Internet navigation program ("browser") or ask any of several powerful search engines (Lycos, Excite, Alta Vista) to search the entire Web for sites that contain a specific topic.

[8] Internet Service Providers ("ISP") are companies that provide access to the Internet such as America OnLine, Compuserve, Microsoft Explorer or any of the smaller commercial, educational or private services. *Id.* at 178. System administrators are individuals who run the private, institutional, governmental or corporate Web-sites visited by computer users who have access to the Web. *Id.* at 189.

[9] A "Personal profile" is an electronic "footprint" analogous to the information a telephone call conveys to the telephone company about the length of a call, its origin and destination but contains nothing about the content of the call.

[10] Jim Erickson, *Are Those Who Go Online to Send Junk Mail Out of Line?,* STAR TRIB., June 30, 1996, at 3D.

information" ("TGI").[11] Such user data can be of value to advertisers and direct marketing services.[12] Although the U.S. government also has access to personal information, legislation based on constitutional rights limits the official use of such data unless good cause is shown.[13] Proposed legislation now seeks to establish guidelines for the private sector's use of personal data—both voluntarily provided and transmission generated—on the Internet and other networks.[14]

This Note examines the issues surrounding the current and possible future uses of transaction generated on-line information and argues for both increased government restrictions and a broadening of the basis for privacy law in order to protect personal privacy within the scope of the U.S. Constitution. Part I explores the capabilities and ramifications of personal electronic data collection in the 1990s. Part II discusses available equitable arrangements and technological interventions designed to control the gathering and use of such data. Part III analyses proposed legislation, current legislation, regulation and case law impacting on

---

[11] *See* ANNE W. BRANSCOMB, WHO OWNS INFORMATION: FROM PRIVACY TO PUBLIC ACCESS 48 (1994); Karen Kaplan, *Caller ID Service Sparks Battle Over Privacy,* L.A. TIMES, Feb. 25, 1996, at A22; *see also* Notice of Inquiry: Privacy Issues Relating to Private Sector Use of Telecommunications-Related Personal Information, 59 Fed. Reg. 6842, 6845 (Nat'l. Telecommunications & Info. Admin. Dept. of Commerce, Feb. 11, 1994) [hereinafter Telecommunications Privacy Notice] (using the term "Telephone Transmission Generated Information"); Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act,* 69 S. CAL. L. REV. 949, 953-54 (1996) (using the term "communication attributes"); Reidenberg & Gamet-Pol, *supra* note 3, at 112 (using the phrase "information about information").

[12] Robert Hawkins, *Junk E-Mail Problem Growing But Solutions May Be on Way*, SAN DIEGO UNION-TRIB., Aug. 13, 1996, at 3; John Schwartz, *Trail of Crumbs Leads Right to the Cyber-Cookie Jar,* WASH. POST, June 24, 1996, at F19.

[13] *See, e.g.,* Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. §§ 1001-1010) (1994) [hereinafter Digital Telephony Act] (requiring court order before allowing government to intercept calls or access call-identifying information).

[14] Consumer Internet Privacy Protection Act, H.R. 98, 105th Cong., 1st Sess. (1997); Communications Privacy and Consumer Empowerment Act of 1996, H.R. 3685, 104th Cong., 2d Sess. (1996).

personal information privacy. Finally Part IV examines the application of tort and property law principles to the non-consensual use of on-line personal information. This Note concludes that proposed privacy protection legislation should be passed immediately and that an expanded legal doctrine based on tort or property concepts or both is necessary to bolster constitutional rights against the challenge of unauthorized use of on-line TGI.

I. PERSONAL INFORMATION AND MARKETING IN A DIGITAL ENVIRONMENT

Nearly all commercial companies (as well as non-profit entities) are involved in "collecting and maintaining information records" on customers, employees, members and contributors. These companies hope to use that information to the company's benefit.[15] Personal information about potential customers is sought by marketers to develop detailed target profiles even when such information is only transactional—names, addresses and product or service used.[16] The methods used to gather such information can be either active or passive. Active gathering is done through manufacturer's registration or warranty cards, telephone surveys or World Wide Web ("Web")-site entrance registration.[17] Information is also obtained passively, without any consumer action, via telephone, video rental or cable records, credit profiles, and, most recently, on-line TGI.[18] In this section, several types of passive and transactionally acquired

---

[15] Mary G. Jones, *Privacy: A Significant Marketing Issue for the 1990s,* 10 J. PUB. POL'Y & MARKETING 133, 133 (1991).

[16] *Id.* at 134. "The new information technologies have transformed American marketers into voracious users of personal data." *Id. See* Ellen R. Foxman & Paula Kilcoyne, *Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues,* 12 J. PUB. POL'Y & MARKETING 106, 108-11 (1993) (exploring the ethical dilemmas faced by marketers as they use TGI without a consumer's knowledge).

[17] *See, e.g.*, The New York Times, *The New York Times on the Web* (visited Oct. 11, 1996) <http:\\www.nytimes.com\>(requesting personal information such as age, gender, zip code and e-mail address before allowing registration for the *New York Times'* free on-line service).

[18] *See generally* Freiwald, *supra* note 11, at 954-57.

information are described and the pros and cons of their use in marketing are considered.

A. *Transaction Generated Information*

TGI is distinguished from content-related computer information. While content-related information includes the text, data and electronic mail ("e-mail") address sent via telecommunications channels (telephone lines via modem, cellular or satellite access),[19] TGI is transmission-related because it is merely a summary of the electronic transmission itself.[20] This information is retrievable and can be sold to marketing companies[21] who assert that they will be better able to target a particular consumer's preferences or interests.[22] This Note considers several types of TGI including

---

[19] *See* Freiwald, *supra* note 11, at 956-58.

[20] *See* Kaplan, *supra* note 11, at A22.

[21] *See* Hawkins, *supra* note 12, at 3 (suggesting that third parties have been compiling mailing lists and consumer profiles based on cookies); Mark Van Name & Bill Catchings, *Web Security and the Cookie Controversy*, PC WK., July 29, 1996, at N6 (positing that addresses could be sold to vendors). *See also* Barry Cooper, *Concern Over Privacy Is Growing on Internet,* ORLANDO SENT., Aug. 31, 1996, at E1 (explaining that "profiles" can be packaged with phone directory and local court information and sold to advertisers and merchandisers).

[22] *See* Erickson, *supra* note 10, at 3D (using the term "clickstream data" for this type of information and calling the electronic tracking and compiling of consumer tendencies "shoppergraphics"). "Advertisers and site operators insist there is nothing insidious in their motives. . . . One of the perceived advantages of the Internet over traditional broadcasting and print mass media is that information, including advertising can be customized for every individual." Erickson, *supra* note 10, at 3D. "'This is not advertising and information as the average consumer has ever known it . . . . These are a set of technologies designed to get to know you intimately, to get to know what makes you think, what makes you respond, and what makes you buy.'" Erickson, *supra* note 10, at 3D (quoting Jeff Chester, Director of the Center for Media Education in Washington, D.C.); Whit Andrews, *Sites Dip Into Cookies to Track User Info*, WEB WK., June 3, 1996, at 17 (calling cookies "a device that will deliver to users the benefits of a site's knowing who they are and what they like"); *see also* Phillip E. Broadbent, *Measuring "Stat Ware" for Site Evaluation: The Best Statistical Programs Offer Click-Stream Analysis, Customizable DB Queries,* DIRECT MARKETING NEWS, Aug. 5, 1996, at 24 (stating that the best Web-site statistics are especially valuable to direct marketing companies because they let them see every move

"cookie" file information,[23] Web server administration information,[24] intelligent transportation information[25] and telephone transmission information.[26]

1. Cookies and Related Data

One specific kind of file that has been publicized recently is Persistent Client-Side HyperText Transfer Protocol ("HTTP")[27] files or "cookie" files.[28] "Cookies" are user files that are currently supported by the Netscape 3.0 browser.[29] When a Web-site is visited, the server can write a file onto the user's computer hard-drive which characterizes what took place at the site.[30] In general,

---

customers make).

[23] *See infra* Part I.A.1 (discussing cookie files and related kinds of data).

[24] *See infra* Part I.A.2 (discussing Web server administration information).

[25] *See infra* Part I.A.3 (discussing intelligent transportation data technology).

[26] *See infra* Part I.A.4 (discussing telephone transmission information).

[27] HyperText Transfer Protocol ("HTTP") is the "language" Web browsers and Web servers use to communicate. *See* CRICKET LIU ET AL., MANAGING INTERNET INFORMATION SYSTEMS 287 (1994).

[28] *See* Al Berg, *Cookies Nibble at Your Disk Drive*, LAN TIMES, July 8, 1996, at 85 (describing cookies as files that Web-sites create and which contain information transferred to or from the Web-site); James Hannaham, *Microchips Ahoy! New Advertisers Track Your Crumbs*, VILLAGE VOICE, Aug. 20, 1996, at 22 (calling the information cookies impart a "minuscule factoid" about the Web-site visitor); Hawkins, *supra* note 12, at 3 (defining a cookie as a small file that contains a profile of a user and his or her computer); Stephan Somogyi, *Web-Based Advertising Is the Same as for Other Media, Only Different*, DIGITAL MEDIA, May 31, 1996, at 11 (stating that cookies provide the capability for individuals to be remembered between viewings of a Web-site); Van Name & Catchings, *supra* note 21, at N6 (pointing out that only the Web-site that placed the cookie is supposed to be able to retrieve it from the viewer).

[29] Netscape Communications Corporation is a producer of software programs including browser programs, such as Netscape Navigator, that display information obtained from the Internet.

[30] Cookies can be used in combination with other information available to the Web server such as "user authentication" to track particular users as they navigate the Web. *See* Eamonn Sullivan, *Are Web-Based Cookies a Treat or a Recipe for Trouble?*, PC WK., June 24, 1996, at 91 (providing a description of the relationship between "targeted marketing" companies that place cookies and the advertisers).

cookies allow sites to "tag" their visitors with unique identifiers so they can be identified each time they visit.[31] One commentator equated cookies to the notion of "a store being able to tatoo a bar code on your forehead, and then laser-scan you every time you come through the doors."[32] Although the processing of this data is currently fairly unsophisticated,[33] the information can be used in conjunction with other files to show what computer you are using, its unique Internet address, the duration of the contact with a Web-site, what specific pages of a site were visited and what electronic transactions were made.[34] Such transactions include

---

A "cookie" is a "calling card that reveals where you're coming from, what kind of computer you have, and many other details. Most sites keep logs of all visitors." Center for Democracy and Technology, *CDT Privacy Demonstration Page* (visited Sept. 13, 1996) <http://www.13x.com/cgi-bin/cdt/snoop.pl> [hereinafter CDT Privacy Page] (on file with *Journal of Law and Policy*). The CDT Privacy Page provides the following readout each time the page is visited:

> Hi! This is [w]hat we know about you:
> Your computer is a _____ running _____.
> Your Internet browser is _____.
> You are coming from _____.
> I see you found this page using the _____ search engine (and I know what you were searching for, too!).

Id.

[31] Andrews, *supra* note 22, at 17. *See* Hannaham, *supra* note 28, at 22 (likening the process to tagging caribou).

[32] John Hilvert, *Bitter Cookies with Java: Just How Anonymous Is Your Surfing?* (visited Sept. 13, 1996) <http://www.pcuser.com.au/privacy.html>(on file with *Journal of Law and Policy*) (quoting Journalist Simson Garfinkel). "'Stores can also read each other's bar codes if they happen to be in the same mall . . . .'" *Id.*

[33] Erickson, *supra* note 10, at 3D.

[34] *See Public Workshop on Consumer Privacy on the Global Information Infrastructure*, ch. II (July 1996) (visited Feb. 10 1997) <http://www.ftc.gov/-www/bcp/conline/pubs/privacy> (on file with *Journal of Law and Policy*) [hereinafter FTC PRIVACY REPORT] (citing that a Web-site "can 'know' users' e-mail addresses, the names of their browsers, the type of computer they are using and the URL or Internet address, of the site from which they linked to the current site"). *See also* Hilvert, *supra* note 32, at <http://www.pcuser.com.-au/privacy.html> (stating that during a visit to a Web-site a log can be recorded which includes a user's Internet Protocol ("IP") address and possibly how long the user was online and what actions the user took).

purchases or requests for further information.

A program that "reads" cookies may be employed to build a database of information.[35] Technology will undoubtedly enable marketing companies to target a specific user with individual offers or advertisements tailored to his or her unique past interests and behavior.[36] The user may not be aware that the gathering of this information is taking place, although there is a proposal to require Web-sites to carry a logo which states that information is being tracked or made available to third parties.[37] Other types of user data gatherers include: the Oil Change program which produces a tailor-made list of items found on various hard drives;[38] Click Stream Data which compiles a list of what items on a Web page have been clicked on;[39] and DoubleClick which receives information from cookie-like files and is thereby able to send unique advertisements to an advertisement window each time a page is visited by the same person.[40] Thus, cookies and related technologies are able to "harvest" information about a subject without any action or approval on the subject's part. In addition to enacting legislation that prevents these secondary uses of personal information, our country must also acknowledge and codify some sort of right to ownership and control of the information in order to fundamentally protect it.

---

[35] Hawkins, *supra* note 12, at 3; Van Name & Catchings, *supra* note 21, at N6; CDT Privacy Page, *supra* note 30. Computer logs can be used for marketing purposes by tying together on-line profiles of users with other publicly available information to develop "rich market data." Freiwald, *supra* note 11, at 958. *See* Broadbent, *supra* note 22, at 24 (explaining new technology that records each user's unique IP address in a database and which is a "far more advanced way[] of tracking this information" than using cookie files).

[36] *See* Hawkins, *supra* note 12, at 3.

[37] eTRUST (project sponsored by Electronic Freedom Foundation). *See infra* Part II.C, note 111 and accompanying text (discussing eTRUST and other non-governmental methods of addressing usage of personal information).

[38] Todd Copilevitz, *Oil Change Renews On-Line Privacy Fears,* GREENSBORO NEWS & REC., Aug. 12, 1996, at D2.

[39] Erickson, *supra* note 10, at 3D.

[40] Ed Foster, *Can Mixing Cookies with Online Marketing Be a Recipe for Heartburn?,* INFOWORLD, July 22, 1996, at 54. "'All we're using it for is to keep track of which ads we've shown you so you don't keep seeing the same one.'" *Id.* (quoting CEO and President of DoubleClick Kevin O'Connor).

2. *Server Administration Data*

Each server has a system administrator who can monitor the TGI of all users who visit the site.[41] Usually such capability is designed to enhance monitoring of system efficiency or security.[42] Site administrators or "Web Masters" can have access to logs of server usage and user information including length of time logged on, particular pages visited or downloaded, type of browser used and the user's IP address.[43] Although many administrators pledge privacy to their subscribers, some could be lured by financial compensation offers from marketers.[44] At the very least, legislation is needed immediately to limit the potential unauthorized uses of such information. However if an individual right in personal information was recognized in general, misuse of such information would be minimized.

3. *Intelligent Transportation Data Technology*

Intelligent Transportation Data Technology that picks up transmissions from vehicles or remote sites on roadways is being increasingly used to track whole fleets or individual vehicles.[45] This technology provides information concerning security,

---

[41] Interview with Richard Jagric, System Manager, Brooklyn Law School, in Brooklyn, N.Y. (Sept. 12, 1996).

[42] *Id. See* Freiwald, *supra* note 11, at 958 (stating that electronic service providers maintain information on their customers' usage and that such logs can be used "in the event that a visitor to a system harms it").

[43] Interview with Richard Jagric, *supra* note 41. *See* LIU ET AL., *supra* note 27, at 316-17. There are several tools available to help the administrator analyze activity. These include "getstats," "wwwstat," "wusage" and use information from "httpd logs" that include: the host name, the date and time and the URL—Web-site address—request. *Id.*

[44] Bill Mann, *Stopping You Watching Me,* INTERNET WORLD, Apr. 1997, at 44 (discussing the possibility of such a sale).

[45] *See* Dorothy J. Glancy, *Privacy and Intelligent Transportation Technology*, 11 COMPUTER & HIGH TECH. L.J. 151, 153 (1995) (discussing the use of such technology to track the weight, speed, tailpipe emissions, worn tires, brakes and even specific driving patterns of vehicles).

maintenance, road conditions and whereabouts.[46] It is also currently used in toll booths to deduct payment from an account without the vehicle having to stop.[47] Although this is a voluntary system, information about a traveler's location can be used to pierce an alibi or establish a pattern of travel without the direct knowledge of the traveler.[48]

> The information that would be generated in an [Intelligent Transportation System ("ITS")] environment would be of interest primarily to law enforcement authorities and commercial marketers[] . . . who are interested in developing profiles of individual habits, patterns, and life-styles [and] regard information resulting from the ITS as a key component of an individual profile that has not been easily documented before.[49]

Without the guidance and limitations of legislation and a grounding of privacy principles in individual rights, secondary uses that encroach on personal privacy will inevitably be made of this technology, as well.

---

[46] *See* Sally Katzen, *Statement Before the House Banking and Financial Services Subcomm. on Domestic and International Monitoring Policy,* FED. NEWS SERV., Oct. 11, 1995, § II(C)(4), *available in* LEXIS, News Library, Fednew File (reporting on the findings of various public forums gathering information on the government's role in protecting the "National Information Infrastructure" and explaining the uses and potential misuses of this technology). "Such systems may also help monitor traffic patterns and road conditions through cameras or other sensors, and provide drivers with information in their cars about the quickest route." *Id.*

[47] *Id.* For example, in New York State the E-Z Pass system is used to automatically deduct tolls from drivers' credit cards.

[48] *See, e.g.,* Phil Agre, *Highway Tolls and Privacy,* 5 PRIVACY FORUM DIG. 3, ¶ 2 (June 1, 1996) <http://www.vortex.com/privacy.html> (citing a story from Agence France Presse on August 17, 1993, reporting a northern French town mayor's alibi being punctured by the lack of evidence that his car passed through a toll). *See also* Glancy, *supra* note 45, at 153-54 (discussing how such information can be used by third parties such as law enforcement agents, private investigators, advertisers and stalkers).

[49] REGAN, *supra* note 6, at 142.

4. *Automatic Number Identification*

Originally used by telephone companies to identify a caller for billing purposes when transferring a call to another network, caller identification ("Caller ID")[50] was later offered as a service to customers and became controversial.[51] Despite the current regulations on Caller ID services,[52] the Federal Communications Commission ("FCC") allows companies who are called on an "800" or "900" number to add the caller's number to their database of customers without informing the caller.[53] This identifier can also be used to get further information on the caller such as address, income level and recent purchases that can then be sold to telemarketers.[54] Again it is apparent that such personal information is susceptible to unauthorized uses without the proscriptions of legislative and judicial doctrines.

B. Direct Marketing

Currently, there is a conflict raging about the ultimate value of direct marketing. There is little doubt that marketing has a positive effect on the sales of products, especially when campaigns are

---

[50] "Caller ID" is defined as automated number identification in which the calling number is displayed. BRANSCOMB, *supra* note 11, at 43.

[51] The central issue in the controversy is whose privacy should be given the most protection—the caller or the one called. GINI G. SCOTT, MIND YOUR OWN BUSINESS: THE BATTLE FOR PERSONAL PRIVACY 346 (1995). Those making the calls do not want their privacy violated especially if they are calling a hot line anonymously versus those who see the identification as a crime deterrent or investigative tool. *Id. See* BRANSCOMB, *supra* note 11, at 44 (citing a Harris poll which found 55% of respondents for regulation of Caller ID, 25% who wanted it banned completely and only 13% in favor of no regulation at all).

[52] Telephone Consumer Protection Act of 1991, 47 U.S.C. § 1002 (a)(2) (prohibiting call-identifying information from being released to the government without a court order or other lawful authorization and from containing information which discloses the physical location of the caller).

[53] SCOTT, *supra* note 51, at 346.

[54] SCOTT, *supra* note 51, at 346.

targeted toward a particular group.[55] Yet surveys show that Americans mistrust marketing companies and feel that information in the marketers' hands is not secure.[56] As more and more people use the Internet and other networks for commercial activities, direct marketing is being used on-line. According to the Direct Marketing Association ("DMA"),[57] more than half of direct marketers are using the Internet and the Web for advertising and forty-eight percent are "mining the membership rosters of major computer online services for e-mail addresses."[58] TGI represents a source of

---

[55] SCOTT, *supra* note 51, at 318 (noting that targeted contacts increase sales by 5-10% while non-targeted marketing only increase sales by 1-2%).

[56] *See* JOHN M. CARROLL, CONFIDENTIAL INFORMATION SOURCES: PUBLIC AND PRIVATE 51 (2d ed. 1991) (citing a 1990 poll commissioned by Equifax, carried out by Louis Harris and Associates and audited by Alan Weston, noted privacy expert and Columbia Law School professor, that found that of nine institutions--including employers, telephone companies and credit bureaus--direct marketing firms engendered the least amount of trust). A 1994 Harris survey of American's attitudes about privacy and emerging interactive technologies which found that:

> 82% of the respondents stated that they are concerned about threats to their personal privacy; 78% believe that consumers have lost all control over how businesses circulate and use personal information; 76% believe that businesses ask consumers for too much personal information and 70% have refused to give information to a business because they felt it was either unnecessary or too personal.

FTC PRIVACY REPORT, *supra* note 34, at ch. II.B. Another statistic from the survey which is particularly relevant to this discussion is that "51% of the respondents stated they would be concerned if an interactive service to which they subscribed engaged in 'subscriber profiling,' i.e., the creation of individual profiles based upon subscribers' usage and purchasing patterns, in order to advertise to subscribers." FTC PRIVACY REPORT, *supra* note 34, at ch. II.B.

[57] "The Direct Marketing Association ("DMA") is the largest trade association for businesses interested in database marketing with more than 3600 member companies from the United States and 47 foreign nations." The Direct Marketing Association, *The Direct Marketing Association—Reception* (visited Feb. 10, 1997) <http://www.the-dma.org/lobby_pages/lobby-reception.html>(on file with *Journal of Law and Policy*).

[58] Erickson, *supra* note 10, at 3D. Recently, the program for the afternoon session of an "Internet Marketing Seminar" offered at the Montague Institute listed the following session: "Extending Traditional Programs: Cookies and Bulletins, Java and Its Implications, Database Searches and Privacy and Security Issues." Brochure, The Montague Institute, *Internet Marketing Seminar:*

valuable, accurate and inexpensive information that, when made available to marketers, can be a useful and powerful tool. Those who value the marketers' distilling and targeting services are enthusiastic about the possibilities. Those who mistrust marketers are doubly concerned because of the all-encompassing nature of the on-line uses. Ultimately, however, society must choose the nature and the extent of personal information use. Our legal system requires that this standard be articulated through legislative and judicial processes.

1. In Defense of the Use of Transaction Generated Information

In what is characterized as a win-win situation, the direct marketing community claims that consumers want to receive material that is of interest to them and do not want to sift through piles of "junk."[59] The marketers claim that TGI is an effortless way to track consumer preferences and provide additional options.[60] With so much data to choose from on the Internet, cookies are seen as a personalized screening mechanism.[61] Cookies also enable the user to enter a password once and have it

---

Afternoon Session (visited Sept. 13, 1996) <http://www.montague.com> (on file with *Journal of Law and Policy*).

[59] Erickson, *supra* note 10, at 3D. "The holy grail of one-to-one marketing is individual information." Erickson, *supra* note 10, at 3D (citing Kathleen Burke, Director of Marketing and Communications for Internet Profiles Corp., a San Francisco-based company that provides services and software for independent analysis of Web-site usage).

[60] Erickson, *supra* note 10, at 3D (citing various marketing companies including, Texas Internet, Internet Profiles Corporation, Juno Online Services L.P. and Fine.com Interactive as well as the DMA. "'People like being called by name, they like having information sorted for them[.] . . . We're not talking about invasion of privacy, we're trying to give people only what they need.'" Erickson, *supra* note 10, at 3D (quoting Dan Fine, Chief Executive of Fine.com Interactive).

[61] Robert Gellman, *They Could Be Watching Your Every Web Move*, GOV'T COMPUTER NEWS, Apr. 29, 1996, at 25. "It is similar to a waiter in your favorite restaurant who remembers what you like to eat. The good part is that you get personal service. The bad part is that someone knows your habits and interests and can tell others." *Id.*

"read" the next time a restricted area is visited.[62] In addition, cookies are a form of the technology that exists behind the "shopping basket" feature of some Web-sites, which enables items purchased and "carried" from different pages or links to be totalled or listed before signing off.[63] Other uses of TGI include new visitor counting,[64] behavior tracking,[65] self-configuring Web pages[66] and "intelligent" information collectors such as PointCast.[67] There is an increasing need for the gathering and

---

[62] Berg, *supra* note 28, at 85.

[63] *See* Berg, *supra* note 28, at 85 (relating the author's experience of using such a "shopping-cart system" to total up an order at a commercial Web-site); Hilvert, *supra* note 32, at 2 (calling such service a "virtual shopping mall"); David Orenstein, *Software Eats Unwanted Web "Cookies,"* ALB. TIMES UNION, Sept. 10, 1996, at E1 (reporting the use of a "shopping basket" system at the on-line book store, Amazon.com).

[64] "New visitor counting" means the page counts not just total number of "hits" or visits but the number of times each individual returns to the page. *Htmlscript Implements "Caller ID" Feature; Simplifies Cookies and Allows HTML Web Developers to Easily Track and Identify Individual Web Browsers,* BUS. WIRE, Sept. 3, 1996, at 1, *available in* LEXIS, News Library, Busdtl File [hereinafter *Htmlscript*]. "HTML" stands for hypertext mark-up language which is the programming language used to create the layout and text on most Web-sites, as of this writing. CRUMLISH, *supra* note 7, at 91.

[65] *See Htmlscript, supra* note 64, at 1. "Behavior tracking" is the process whereby the htmlscript program can track each mouse click while the visitor explores the Web page, providing data to the Web page owner on how users navigate the site. *Htmlscript, supra* note 64, at 1.

[66] *See Htmlscript, supra* note 64, at 1. If a visitor sets Web page configuration preferences (such as background colors and content), they will be remembered and restored each visit. *Htmlscript, supra* note 64, at 1.

[67] Louise McElvogue, *The Web Gains That Personal Touch,* GUARDIAN, July 18, 1996, at 2. PointCast is a service on the Web that provides software which periodically scans the Internet for user specified information and displays updates on news, sports and other areas of interest when the computer is turned on. *Id.* It is able to "learn" other areas of user interest by tracking Internet travels. *Id.* Several other products are also able to "narrowcast" or deliver a custom experience for each viewer. *Id.* The *Wall Street Journal*'s Personal Journal and the *New York Times*' Clipper service capture only the type of news reports requested by the subscriber. *Id.* Firefly is another service on the Web that selects content for its users. It uses "agent technology" to seek out other net users with similar tastes and "learns" more about the user's preferences depending on how the user responds to the information. *Id. See generally* Kevin Kelly & Gary

sorting of information from the Internet. Without individualized "screening" mechanisms, one can easily experience information overload and be less able to use the wealth of knowledge that exists on-line.

In addition, the American marketing community claims that if restraints are put on the commercial use of the system, it will not survive, spelling the loss of the promise of global interconnectedness.[68] It is because the United States lacks privacy restraints that it has been able to assume world leadership while the Europeans have embraced such laws and are not able to compete.[69]

Finally, an economic argument is made that the ease and efficiency of marketing in the electronic age will decrease transaction costs which will be beneficial to society.[70] For example, corporations will be able spend more time marketing to those who truly are interested in their products; interested consumers can acquire more information and others will not waste time sifting through unsolicited electronic mail.[71]

In sum, the defenders of the free use of personal information see the minimal loss of anonymity as well worth the individual and societal benefits of easier information access.

2. *In Fear of the Uses of Transaction Generated Information*

To privacy advocates, however, the release of information without one's consent represents a serious breach of privacy,

---

Wolf, *Push: Kiss Your Browser Goodbye: The Radical Future of Media Beyond the Web*, WIRED, Mar. 1997, at 12 (describing this new type of technology that is called "push" technology because it is information that is pushed to the user rather than what the user finds by actively searching the Internet); Niel Robertson, *A Personalized Web*, INTERNET WORLD, Apr. 1997, at 32-34 (discussing push and agent technology).

[68] Robert Posch, *A Serious Nation Validates Itself in Serious Challenges: Privacy*, 58 DIRECT MARKETING 46, 48 (Nov. 1995) (arguing that our society has chosen to give up some privacy in return for the economic freedoms that have given the United States "a monopoly on the information economy").

[69] *Id.* at 49 (stating "no greater regulatory burden could be imposed on an information economy than burdensome, pointless privacy regulations").

[70] FTC PRIVACY REPORT, *supra* note 34, at ch. I.

[71] FTC PRIVACY REPORT, *supra* note 34, at ch. I.

especially when the information concerns where one has traveled (on-line or "on the road"), how long one has visited and what transactions took place.[72] Without controls, they argue, additional uses could be made of such information that could conflict with a person's interests or desires. For example, summaries of on-line interests could be sold to direct marketers who would then initiate a direct e-mail or "snail mail" (regular mail) campaign.[73] More significantly, medical status might be inferred from Web interests and used to disadvantage an individual if provided to a medical insurer or employer.[74] In addition, interests in certain sites could lead to inferences about a person's religious, political or sexual preferences that might also be used against them.[75] Therefore, the security of such information is of great concern. In addition, when personal information is obtained without knowledge or consent not only is there an affront to individual integrity but it threatens the use of the system itself. A lack of confidence in the network causes

---

[72] *See* Steve Ulfelder, *Online Snoop!: Editor Turns Electronic Gumshoe, Digs Up Dirt—On Himself*, COMPUTERWORLD, Aug. 12, 1996, at 82. *See also* PERRITT, *supra* note 2, at 147 (arguing that "the possibility that some enterprises . . . may make money by collecting consumer transaction data and selling the 'click stream' implicates major personal privacy concerns"). *See generally* CDT Privacy Page, *supra* note 30 (providing information on electronic privacy concerns and links to other privacy Web-sites such as the Electronic Freedom Foundation and the Electronic Privacy Information Center).

[73] CDT Privacy Page, *supra* note 30 (noting that, although one might not be concerned if such a campaign resulted in a free sample, coupons, or e-mail regarding tobacco products, for instance, if visits to tobacco Web-sites resulted in escalating insurance premiums due to categorization as a smoker there might be reason to worry).

[74] Judith B. Prowda, *A Lawyer's Ramble Down the Information Super-Highway: Privacy and Security of Data,* 64 FORDHAM L. REV. 738, 742 (1995). "Of all the types of information collected about individuals, the public is most troubled by the prospect of unauthorized disclosure of medical . . . information." FTC PRIVACY REPORT, *supra* note 34, at ch. 2.D. (citing the testimony of Professor Alan Westin). *See* Jones, *supra* note 15, at 134 (noting the possibility that insurance companies and employers can use prescreening and database matching to identify "individuals whose costs exceed the norm or whose life-styles are such as to mark them as likely candidates for certain types of illnesses").

[75] *See* Freiwald, *supra* note 11, at 959 n.37 (describing how searches could be run on keywords such as "abortion," "communist" or "homosexual").

a "crisis of confidence" in providers of communication and communication entrepreneurs themselves.[76] Providers understand that short-term benefits could turn into long-term problems if consumers discover how information is being used and react negatively toward a company.[77] Although companies may seek access to consumer information, they do not want their own corporate information made available on the network.[78] Finally, without an enforceable standard of security and reliability, these services will lose participants and commerce will be threatened.[79]

Increasingly, as foreign countries that restrict the use of personal information refuse to trade with a country whose standards are insufficient, global commerce will also be jeopardized.[80] For example, the European Union Privacy Directive states that:

> Member States shall provide that the transfer to a third country of personal data which are undergoing processing

---

[76] Reidenberg & Gamet-Pol, *supra* note 3, at 122 (for example, if a company is tracking female wig buying or male fashion underwear purchases).

[77] Reidenberg & Gamet-Pol, *supra* note 3, at 122. For example, in January 1991, Lotus and Equifax, a credit bureau, planned to release "Marketplace," a CD-ROM which revealed detailed information on the shopping habits of 120 million Americans. CARROLL, *supra* note 56, at 163-64. The program was withdrawn as a result of protests from the American Civil Liberties Union ("ACLU") and consumer activists. CARROLL, *supra* note 56, at 164.

[78] Reidenberg & Gamet-Pol, *supra* note 3, at 122 (citing the loss in confidence when the Clinton administration proposed the Clipper Chip standard of security that took control away from individual corporations).

[79] Reidenberg & Gamet-Pol, *supra* note 3, at 122-23.

[80] *See* Reidenberg & Gamet-Pol, *supra* note 3, at 123 (discussing the lack of "global interoperability" between the European Communities ("EC") and the United States); *see also* Reidenberg, *supra* note 4, at 240-41 (reviewing EC privacy policies as well as that of several individual European nations); Electronic Privacy Information Center, *A Review of the Proposed Principles of the Privacy Working Group* (visited Sept. 6, 1996) <http://www.epic.org> (on file with *Journal of Law and Policy*) (stating that "the proposed privacy principles will be considered inadequate by most European countries because the principles provide insufficient protection for personal data"). *See generally* COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES (1992) (comparing the development of privacy doctrines in Europe and the United States and questioning whether harmonization will be possible).

> or are intended for processing after transfer may take place only if . . . the third country in question ensures an adequate level of protection.[81]

If the third country does not meet this "adequacy" standard the "Member States shall take the measures necessary to prevent the transfer of data of the same type *to* the third country in question."[82] Therefore, consumers, businesses and international communities are arguing for immediate legislative action and judicial guidelines to protect the use of personal information.

3. Society's Choice

The societal issues raised by such opposing views, although familiar, are of a wholly new order in the digital age. While some argue that electronic intrusions into the private sphere are not harmful in nature,[83] are freely available from other sources[84] and, in fact, may be beneficial,[85] the existence of instantly available and transactionally generated personal information completely changes the scope of the issue. As the use of cookie files and related technologies increase, so too will public debate about

---

[81] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Eur. O.J. L281/31 (Nov. 23, 1995). The International Electronic Rights Server, *Privacy International* (visited Feb. 11, 1997) <http://www.privacy.org/pi/intl_orgs/ec/dp_directive_-final.txt> (on file with *Journal of Law and Policy*).

[82] *Id.* (emphasis added).

[83] Robert Brueckner, *"Cookies" Will Crumble Without Value; The Real Opportunity: Cultivating One-on-One Relationships,* DIRECT MARKETING NEWS, Sept. 23, 1996, at 18. Despite the plethora of information obtained from cookie files, it is largely descriptive of the entire Internet-surfing population and not specific to any individual. *Id.*

[84] Credit reports and credit cards, for example, give much information about interests and travel through purchase histories. Reidenberg & Gamet-Pol, *supra* note 3, at 121-22 (obtaining records of credit card purchases, magazine subscriptions and public information, however, are not without time- and resource-consuming efforts that increase the cost of obtaining such information).

[85] *See supra* Part I.B.1 (discussing the positive aspects of using TGI).

whether and to what degree such intrusions should be regulated.[86] In resolving this conflict, society must make fundamental decisions about the privacy principles that will guide technology and communications into the twenty-first century. It is yet another opportunity to lay the legal groundwork for a comprehensive privacy policy—guidance this country has never enjoyed.

II. EXTRA-LEGAL REMEDIES AND CONTROLS

Although current law does not directly regulate the use of personal information by private industry,[87] there are several "extra-legal"[88] options that can impact on the uses of such information. These include industry self-regulation, technological "fixes" and a free market or economic approach.

A. Industry Self-Regulation

Information businesses have a large stake in protecting the privacy of communication networks generally. This not only includes maintaining the confidence of their customers but also protecting the security of their company's information.[89] Selfregulation can take the form of explicit codes of company

---

[86] *See, e.g.*, FTC PRIVACY REPORT, *supra* note 34, ch. I (discussing the challenges facing consumers, institutions and the government in the area of privacy and technology).

[87] *See infra* Part III (discussing the legal remedies which address personal privacy). *See also* Freiwald, *supra* note 11, at 950-51 (stating that the disclosure of "communication attributes"—TGI—is protected more weakly, if at all, than is the content of communications).

[88] The term "extra-legal" means outside the legal-legislative system.

[89] Paul M. Alberta, *DMers Told They Could Be Driven Out of Business Over Privacy Issue*, DIRECT MARKETING NEWS, Apr. 5, 1993, at 7 (citing a speaker at the 28th annual spring conference of the Direct Marketing Association stating "[e]ither we regulate ourselves or we shall be regulated out of business with only ourselves to blame"). "There is always the possibility of being legislated virtually out of existence by the Federal Trade Commission. . . . The privacy issue is going to be very sensitive, and invasion of privacy legislation could virtually destroy our new information-gathering techniques." *Self-Policing Needed To Stem Legislative Tide*, MARKETING NEWS, Aug. 2, 1985, at 13 (quoting the President of Speigel, Inc.).

conduct, actual contracts with consumers or informal norms and business practices.[90] In addition, influence from outside groups[91] may promote "good citizenship" standards. But problems arise in this area because most self-regulation programs are not legally binding and there are few enforcement mechanisms. Even when a company has a policy, it is not obligated to reveal it to the public,[92] and usually will not, unless there is a marketing or publicity advantage to be gained.

The Direct Marketing Association has established guidelines for its members that promote consumer control over their own information.[93] In other contexts, the industry has recommended that members honor requests from consumers not to reuse information.[94] However, not all marketers are members of the DMA.[95] A recent trade article suggests that despite the ease of both obtaining information by way of TGI, and marketing information via "d-mail" (direct e-mail), restraint should be practiced in order to prevent the alienation of potential clients.[96]

---

[90] For example, both American Express and Chase Manhattan have codes that prohibit the disclosure of customer records to third parties, and Chase assumes an obligation to limit internal use of its customers' files to employees directly involved. Jones, *supra* note 15, at 31.

[91] For example, the ACLU, the Electronic Privacy Information Center, the Center for Democracy and Technology or the Electronic Freedom Frontier are among such groups.

[92] *See* Reidenberg & Gamet-Pol, *supra* note 3, at 120.

[93] The Direct Marketing Association sponsors both a mail and telephone "preference service" that will remove a customer's name from a central mailing list upon request. *See* SCOTT, *supra* note 51, at 320.

[94] SCOTT, *supra* note 51, at 320.

[95] Another group to which many on-line marketers belong is the Interactive Services Association, a 16-year-old association that promotes and develops "consumer interactive services" worldwide. Interactive Services Association, *Guidelines for Online Services* (visited Feb. 10, 1997) <http://www.isa.net/-about/whatisa.html>.

[96] Brueckner, *supra* note 83, at 18. Once alienated by and alerted to the effects of "d-mail" (direct e-mail), customers will start refusing the cookies and "they'll investigate and invest in 'cookie-cutter' technology. Already, mail-filtering software has the ability to scuttle even the best d-mail effort. And more is on the way." Brueckner, *supra* note 83, at 18. *See infra* Part III.B (discussing these technologies).

On-line service providers also police themselves and, in fact, many already have privacy clauses in their provider agreements.[97] A Web consortium called "W3" has been established as an "official standards body" with a focus on gathering user demographic information.[98] In addition, I/CODE, a commercial "universal registration system," bills itself as a solution to "gathering valuable demographic data on visitors" and provides an incentive-based program to customers who voluntarily give personal information.[99] The program explicitly states that it will "never disclose any I/CODE member's identity or personal contact information without the user's explicit authorization."[100]

Thus, although there is a general acceptance by commercial and marketing enterprises of the need for self-regulation, lacking mandates or guidance from government, there is little agreement on a universal system that can meet the needs of diverse industries, as well as consumers.

B. Consumer Self-Help Technology

Filling the void in regulation, entrepreneurs have begun to create products that can block TGI from remote viewers. These include dedicated software such as Internet Fast Forward,[101] NSClean32[102] and Web Filter.[103] Netscape has added an

---

[97] Center for Democracy and Technology, *Privacy Policy Chart—Online Service Providers* (visited Mar. 19, 1997) <http://www.cdt.org/privacy/-online_services/chart.html>.

[98] The World Wide Web Consortium, *Proposals for Gathering Consumer Demographics* (visited September 13, 1996) <http://www.w3.org/pub/WWW/-Demographics/>. *See infra* Part II.B (discussing the Consortium's program).

[99] *I/PRO, I/CODE: A Universal Registration System* (visited Sept. 23, 1996) <http://www.icode.ipro.icode_ corporate_site//>.

[100] *Id. See* FTC PRIVACY REPORT, *supra* note 34, at ch. III.A.1 (describing I/PRO as an example of a universal registration system).

[101] *See* Berg, *supra* note 28, at 87 (explaining that Internet Fast Forward will filter cookies and advertising graphics).

[102] *See* Orenstein, *supra* note 63, at E1 (describing software that gives out false e-mail addresses as users visit sites).

[103] *See* Laura Rich, *Overriding Web Ads,* INSIDE MEDIA, May 15, 1996, at 27 (describing Fast Forward's competitor WebFilter which requires users to

adjustment to its 3.0 Browser that, when configured correctly, warns the user that a remote site is placing a cookie file.[104] The user can then prevent the cookie from being given. However, it is important to note that not all users have 3.0 and that the default setting on the browser is to not warn of the cookie.

Another technique used to protect information is to make the information useless to commercial concerns. One means of achieving this status is to use a server that allows anonymous Web surfing such as The Anonymizer.[105]

The World Wide Web Consortium at the Massachusetts Institute of Technology developed a Platform for Internet Content Selection ("PICS") to enable parents to block their children's access to certain Internet sites[106] via a rating system similar to that being designed for television. However, such a system can also be used to enhance privacy by way of a rating system based upon the "privacy-protectiveness" of the Web-site. The desired level of protection could be set individually, thereby allowing a person who is not concerned about giving out personal information to visit all sites, while another might want to restrict Web wanderings to only those sites that have pledged to not divulge personal information without permission.[107] In a similar vein, a third approach to the lack of privacy regulation is a free market philosophy.

C. Free Market

If no regulation is imposed, either internally or by the government, economic forces presumably will act on the information flow to enable consumers to choose the level of privacy they would forgo in return for compensation of a sort.[108] In one experiment

---

designate pages it wants to be ad-free).

[104] Sullivan, *supra* note 30, at 75.

[105] *See* The Anonymizer, *Anonymous Surfing* (visited Sept. 13, 1996) <http://www.anonymizer.com> (service that allows Internet communication "without revealing any personal information").

[106] FTC PRIVACY REPORT, *supra* note 34, at ch. III.A.3.

[107] FTC PRIVACY REPORT, *supra* note 34, at ch. III.A.3.

[108] *But see* REGAN, *supra* note 6, at 228 (arguing that "three factors limit the effectiveness" of such an approach: 1) the contradictory interests of third party

in West Covina, California, a shopping mall provided an incentive to shoppers to provide the mall stores with personal data.[109] Those that gave information on their income and spending were eligible for prizes amassed from the sale of the information to direct marketing companies.[110] In a sense, these consumers realized the value of their personal information and knowingly risked their anonymity in a lottery for a chance to get a greater return.

In the on-line world, the Electronic Frontier Foundation, a San Francisco-based Internet watchdog organization, is starting a world-wide campaign in which participating Web-sites will reveal their privacy policies via different logos called "trustmarks."[111] This program, known as eTRUST, has been developed to inform users whether personal information is being collected, and if so, whether it will be released to third parties.[112] In this way, consumers can make informed choices about whether they wish to continue visiting a site where their personal information is not secure.

---

information holders; 2) the "nonvoluntary nature" of many consumer-information holder relationships; and 3) technology).

[109] SCOTT, *supra* note 51, at 322. After filling out applications asking for personal information such as "addresses, the ages of family members, income level, reading habits and plans to purchase cars or jewelry," participants received Plaza Players Club cards that, when inserted into automatic teller machines at the mall, made them eligible for weekly prizes such as $500.00, vacations, gifts and discount coupons. SCOTT, *supra* note 51, at 322. Although there was an initial fear from privacy advocates that the information would be sold to marketers outside the mall, "the data was kept in the mall, and most consumers found the program beneficial." SCOTT, *supra* note 51, at 322. "They were quite willing to give up the information asked with the understanding that this data about their buying habits might be sold in return for the possibility of various awards . . . ." SCOTT, *supra* note 51, at 322.

[110] SCOTT, *supra* note 51, at 322.

[111] The eTRUST, *eTRUST On-Site Information Page* (visited Nov. 27, 1996) <http://www.etrust.org/onsite.html>. eTRUST has three tiers which can be chosen by program participants: (1) No Exchange—"insures anonymous usage, anonymous transactions, anonymous chat and anonymous tracking;" (2) One to one Exchange—ensures "that the services will not disclose individual or transactional data to third parties;" and (3) Third Party Exchange—"informs the user that the services will be disclosing information to third parties." *Id.*

[112] *See* Orenstein, *supra* note 63, at E1.

These models, however, assume that people are free to contract voluntarily. In fact, obtaining personal information from a network without a customer's knowledge is not a voluntary arrangement. The individual is not technically a party to the exchange. Most importantly, "it is not in the interests of the third party record keepers to give people complete information . . . because it would lower the value of their product if people denied organizations the ability to use personal information as a commodity."[113]

Whether on not the inequities in such free market arrangements are resolved, it is clear that consumers and industries are trying to find ways to address privacy questions in the on-line world. Barring the effectiveness of self-regulation, technological self help arrangements and free market solutions, it is likely that citizens will turn to the legal system for ultimate guidance in this volatile area as they have when other technological threats to privacy have arisen.

III. LEGAL REMEDIES

The United States does not have comprehensive privacy rights or principles that address "the acquisition, storage, transmission, use or disclosure of personal information within the business community."[114] As a result, legal protections are enacted through ad hoc legislation or by individual states' common laws.[115] Although various statutes protect individuals from the government's misuse of personal data,[116] there is little legislation of the use of personal

---

[113] REGAN, *supra* note 6, at 228. Given the opportunity to opt out of providing information, only about 20% utilized the option. *See* REGAN, *supra* note 6, at 233. It is estimated that only 5-10% would opt in to giving consent for further uses. REGAN, *supra* note 6, at 233.

[114] Reidenberg, *supra* note 4, at 208. *See* Freiwald, *supra* note 11, at 961 (stating that communication attributes have been afforded weak federal protections versus the strict protection for communication content); Prowda, *supra* note 74, at 751 (stating "there is no omnibus privacy legislation applicable to the private sector").

[115] *See* Reidenberg, *supra* note 4, at 208.

[116] *See, e.g.,* Electronic Communications Privacy Act of 1984, Pub. L. No. 99-508, 100 Stat. 1848 (1986) [hereinafter ECPA] (addressing issues of government surveillance via electronic means); Communications Act of 1934, 47 U.S.C. § 605 (1988) (controlling government wiretapping).

information by the private sector[117] and no underlying philosophy that guides policymaking in this area. Notwithstanding this historical patchwork, two new statutes have recently been proposed that would directly regulate the use of TGI by private entities.[118] The following section analyses previous legislation and common law decisions as they pertain to both the acquisition and dissemination of personal information, and evaluates the current proposals.

Privacy laws are based on a range of legal doctrines.[119] Although the right to privacy is not expressly granted in the U.S. Constitution, the Supreme Court has ruled in favor of various privacy interests, deriving the right to privacy from the First, Third, Fourth, Fifth and Ninth Amendments.[120] Furthermore, ten state

---

[117] *See infra* Part III.C.3 (discussing the Fair Credit Reporting Act); *infra* Part III.C.2. (discussing the Electronic Communications Privacy Act).

[118] The Consumer Internet Privacy Protection Act of 1997, H.R. 98, 105th Cong., 1st Sess. (1997); the Communications Privacy and Consumer Empowerment Act, H.R. 3685, 104th Cong., 2d Sess. (1996). *See infra* Part III.C-D (discussing each act).

[119] Privacy statutes have resulted from legislation as well as common law decisions. *See* Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. §§ 1001-1010) (1994) (restricting usage of telephone transmission information); Katz v. United States, 389 U.S. 347, 353 (1967) (finding a privacy right in a telephone call from a public telephone booth). *See also infra* note 128 and accompanying text (discussing the federal wiretapping statute).

[120] The First Amendment provides:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press, or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

U.S. CONST. amend I. *See* Talley v. California, 362 U.S. 60, 64-65 (1960) (finding a First Amendment "right to anonymity in public expression"); NAACP v. Alabama, 357 U.S. 449, 462 (1958) (finding a First Amendment right to freedom of association); Watkins v. United States, 354 U.S. 178, 187 (1957) (enforcing a First Amendment freedom in political belief).

The Third Amendment provides:

> No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.

U.S. CONST. amend III. The Third Amendment prohibition against quartering soldiers was extended to "a right to privacy against unreasonable surveillance and

constitutions[121] explicitly define personal privacy as a protected and fundamental right, though no two states have the same standard.[122]

---

compulsory disclosure." REGAN, *supra* note 6, at 35.

The Fourth Amendment provides:

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

U.S. CONST. amend IV. There is an individual right as well as a protection against arbitrary government action in the Fourth Amendment. *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (finding a Fourth Amendment right based on the expectation of privacy); Olmstead v. United States, 277 U.S. 438, 465-66 (1928) (finding no privacy interest when no physical trespass was involved). *But see* United States v. Miller, 425 U.S. 435, 440-41 (1976) (finding no Fourth Amendment right in personal bank records that were deemed business records of the bank).

The Fifth Amendment provides:

> No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury . . . nor shall any person be subject for the same offence[sic] to be twice put in jeopardy of life or limb, nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use without just compensation.

U.S. CONST. amend V. A Fifth Amendment privilege against self-incrimination has been used to protect privacy but its application has been limited to criminal cases. REGAN, *supra* note 6, at 38.

The Ninth Amendment provides:

> The enumeration in the Constitution of certain rights shall not be construed to deny or disparage others retained by the people.

U.S. CONST. amend IX. *See* Griswold v. Connecticut, 381 U.S. 479, 484-86 (1965) (finding a penumbra of rights to privacy and ruling a Connecticut statute prohibiting the prescription or use of contraceptives an infringement on marital privacy).

[121] ALASKA CONST. art. I, § 22; ARIZ. CONST. art. 2, § 8; CAL. CONST. art. I, § 1; FLA. CONST. art. I, § 23; HAW. CONST. art. I, § 6; ILL. CONST. art. I, § 6; LA. CONST. art. I, § 5; MONT. CONST. art. II, § 10; S.C. CONST. art. I, § 10; WASH. CONST. art. I, § 7.

[122] Prowda, *supra* note 74, at 739. *See, e.g.*, ARIZ. CONST. art. II, § 8 ("No person shall be disturbed in his private affairs, or have his home invaded, without authority of law."); CAL. CONST. art. I, § 1 (listing privacy as one of the

A. *Privacy From Intrusion—Controlling Information Acquisition*

In *Katz v. United States*,[123] Justice Harlan first articulated the two part test for the application of the Fourth Amendment's search and seizure provisions to privacy cases.[124] First, there must be a subjective expectation of privacy and, second, that expectation must be found reasonable from society's view.[125] Although the objective part of the test was later narrowed to allow only "legitimate" expectations of privacy,[126] the Supreme Court has established a continuum of locations from public spaces (such as fields and highways) to one's home where the expectation of privacy is unquestionably legitimate.[127]

In 1968, after forty years of debate and discussion, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act ("Act")[128] to codify protections and procedures for government wiretapping.[129] This Act covered all aural acquisition of wire and oral communication carried by commercial telephone carriers.[130] The Act was extended by the Electronic Communication Protection

---

inalienable rights).

[123] 389 U.S. 347 (1967).

[124] *Id.* at 361 (extending the expectation of privacy to telephone conversations and invalidating wiretapping without a showing of good cause by the government). In part, this decision was based on the Supreme Court's acknowledgment of the "vital role that the public telephone has come to play in private communication." *Id.* at 352. *But see Olmstead*, 277 U.S. at 466 (holding that there is no reasonable expectation of privacy in telephone calls and thereby allowing wiretapping by the government).

[125] *Katz*, 389 U.S. at 361.

[126] *See* Rakas v. Illinois, 439 U.S. 128, 143 (1978) (limiting expectation of privacy to areas that the law recognizes as "legitimate").

[127] *See* REGAN, *supra* note 6, at 37.

[128] Pub. L. No. 90-351, 82 Stat. 213 (June 19, 1968) (codified at 18 U.S.C. §§ 2510-2520) (1968) [hereinafter Title III].

[129] There were two ostensible purposes for Title III: (1) to protect the privacy of wire and oral communications; and (2) to clarify what had been inconsistent law by establishing uniform national rules. S. REP. NO. 1097, at 66 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2124, 2153-54.

[130] 18 U.S.C. § 2510 (1968).

Act of 1986,[131] to cover the many new forms of electronic communication that had arisen.[132]

In *Smith v. Maryland*,[133] however, the Supreme Court found no expectation of privacy attached to the numbers dialed on a telephone because the caller assumes the risk that the telephone company will reveal them to the police.[134] In dissent, Justice Stewart argued that the numbers have content because they reveal significant details of a person's life, and therefore should be afforded constitutional protection.[135]

The most recent successful effort to protect access to personal information, however, was the enactment of the Driver Privacy Protection Act of 1994.[136] It was a response by Congress to the stalking and murder of an actress whose personal information was revealed via motor-vehicle records.[137] The law is the first legislation that limits access to public records and represents a compromise between individual privacy advocates and the private sector.[138] It allows individuals to "opt out" of allowing information to be given to marketers and others.[139] Privacy advocates, however, sought an "opt in" approach whereby the presumption is

---

[131] Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. § 2510). *See infra* Part II.C.2 (discussing the Electronic Communication Protection Act).

[132] PERRITT, *supra* note 2, at 99. Examples of new forms of electronic communication are: electronic mail operators, computer-to-computer data transmission, cellular and cordless telephones, pagers, video conferencing, communication carried by microwave or fiber optics and digitized voice or video. The Electronic Communication Protection Act was also intended to extend coverage beyond common carriers to private networks. PERRITT, *supra* note 2, at 99.

[133] 442 U.S. 735 (1979).

[134] *Id.* at 743.

[135] *Id.* at 746-48 (Stewart, J., dissenting).

[136] 18 U.S.C. § 2721 (1994).

[137] BRANSCOMB, *supra* note 11, at 25. Rebecca Schaefer was murdered in 1989 by a stalker who obtained her address from "public" motor-vehicle records. BRANSCOMB, *supra* note 11, at 25.

[138] REGAN, *supra* note 6, at 103.

[139] 18 U.S.C. § 2721(b)(12)(A) ("[M]otor vehicle department has implemented methods and procedures to ensure that—individuals are provided an opportunity, in a clear and conspicuous manner, to prohibit such uses . . . .").

total privacy, however, an individual can give permission for his or her name to be given out.[140] The information media and direct marketing industries successfully opposed such an "opt in" provision fearing that similar mechanisms would be required to access other public databases such as voter registration and real estate records.[141] In 1994, the Supreme Court stated that individuals have a "far from insignificant" privacy interest in home address information regardless of the fact that such information may already be in the public domain.[142]

Consequently, an aggregation theory of information accumulation has also been advanced against access to such information.[143] When information is gathered from sources that do not have an expectation of privacy and is combined to give a profile of an individual, the aggregation theory has been used to argue that the information should be protected.[144] In *Nader v. General Motors*,[145] Judge Breitel stated:

> Although acts performed in 'public,' especially if taken singly or in small numbers, may not be confidential, at least arguably a right to privacy may nevertheless be invaded through extensive and exhaustive monitoring and cataloguing of acts normally disconnected and anonymous.[146]

This same principle is behind the 1988 Privacy Protection Act's restrictions on combining data sets,[147] and it is certainly applicable to aggregating TGI.

---

[140] REGAN, *supra* note 6, at 102-03.

[141] REGAN, *supra* note 6, at 102-03.

[142] United States Dep't of Defense v. Federal Labor Relations Auth., 510 U.S. 487, 501-02 (1993).

[143] PERRITT, *supra* note 2, at 147.

[144] PERRITT, *supra* note 2, at 147.

[145] 25 N.Y.2d 560, 255 N.E.2d 765, 307 N.Y.S.2d 647 (1970).

[146] *Id.* at 572, 255 N.E.2d at 772, 307 N.Y.S.2d at 657 (Breitel, J., concurring).

[147] Computer Matching and Privacy Protection Act, 5 U.S.C. § 552a(o) (1988).

The U.S. Court of Appeals for the Eighth Circuit addressed the issue of information aggregation in *Tureen v. Equifax, Inc.*.[148] Although the court found that the defendant-credit bureau did not violate the plaintiff's privacy "merely by collecting and retaining his past insurance history,"[149] it left the door open in its dicta for a cause of action for information that is "highly personal." The court stated, "We do not rule out the possibility that instances may exist where the collection of *highly personal* information, irrelevant to any legitimate business purpose might constitute an invasion of privacy by unreasonable intrusion."[150]

Despite these sporadic attempts to plug holes in private sector access to citizen's personal information, commercial entities continue to be able to obtain such information for "legitimate" uses. Another issue, however, is to what degree the use of such information has been regulated.

B. Privacy From Dissemination—Controlling Information Distribution

Beginning in the 1960s and early 1970s the use of computers, especially large capacity mainframe computers to acquire and store information, created cause for concern about the security of personal information.[151] Not only were Medicare, Medicaid and other government entitlement programs expanding, but private industry, especially the insurance and credit industries, was increasingly using data storage to improve its operations and remain competitive.[152] With the Watergate revelations of "enemy lists" and infiltrations of private citizens, there was a willingness to explore possible legislation to control potential abuses.[153]

---

[148] 571 F.2d 411 (8th Cir. 1978). *Tureen v. Equifax, Inc.* held that the release of 25-year-old insurance information to disability fraud investigators, as part of a credit record, was not violative of the plaintiff's privacy under either the intrusion or private facts tort. *Id.* at 415-17.

[149] *Id.* at 416.

[150] *Id.* (footnote omitted, emphasis added).

[151] REGAN, *supra* note 6, at 8.

[152] REGAN, *supra* note 6, at 69.

[153] *See* REGAN, *supra* note 6, at 126 (discussing the aftermath of the

Several policy groups and conferences were therefore established, including the Privacy Protection Study Commission ("PPSC")[154] and a 1974 Department of Health, Education and Welfare ("HEW") committee.[155] HEW issued a report entitled "Records, Computers and the Rights of Citizens," that pointed to inadequacies in then current laws and policies and recommended the incorporation of the Code of Fair Information Practices.[156] Although it was not made

---

Watergate revelations); Prowda, *supra* note 74, at 744 (explaining how such mistrust spawned subsequent legislation).

[154] Established by Congress to make "legislative recommendations . . . necessary to protect the privacy of individuals while meeting the legitimate needs of government and society for information." REGAN, *supra* note 6, at 83 (citing the Privacy Act of 1974). *See infra* note 158 and accompanying text (discussing the Privacy Act of 1974).

[155] The Secretary's Advisory Committee on Automated Personal Data Systems was set up to "analyze and make recommendations regarding harmful consequences that could result from computerized information systems . . . ." REGAN, *supra* note 6, at 75.

[156] United States Dep't of Health Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* (Washington, D.C.: Government Printing Office, 1973) (cited in 1974 U.S.C.C.A.N. 6916, 6923-24) [hereinafter HEW Report]. According to the recommended but unenacted Code of Fair Information Practices set forth in the Department of Health Education and Welfare ("HEW") Report:

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

Id.

part of any subsequent bill, the Fair Information Practices Code set a standard of information privacy that continues to be debated today.[157]

In 1975, the Privacy Act of 1974 ("Privacy Act")[158] was signed into law. It incorporated recommendations from various governmental hearings and reports on privacy.[159] Two key issues in the hearings and debates prior to passage of the Privacy Act were whether the same legislation should apply to both the public and private sector and whether there should be a Federal Privacy Board to oversee and administrate federal privacy protections.[160] However, due to strong pressure from federal agencies and private industry groups,[161] only public actions were covered by the law and no Federal Privacy Board was put in place.

Although the Privacy Act did not provide a governmental oversight body nor implement the Fair Information Code,[162] it did, however, set important standards for government information handling.[163] It gave individuals the right to know what

---

[157] REGAN, *supra* note 6, at 76-77.

[158] Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified at 5 U.S.C. § 552a (1982 & Supp. V)) [hereinafter the Privacy Act].

[159] *See, e.g.*, HEW Report, *supra* note 156, at 6923-24.

[160] REGAN, *supra* note 6, at 78.

[161] For example, private industry was represented by the American Life Insurance Association and the Department of Commerce spoke on behalf of government agencies. These representatives argued that there was little evidence of abuses in private sector personal information handling and put the burden of proof on privacy advocates to come up with specific examples or actual patterns of abuse. They also complained that the private sector was already overburdened by regulation. REGAN, *supra* note 6, at 78. Additionally, they said that the private sector would be able to "self-regulate" to protect consumers. REGAN, *supra* note 6, at 78.

[162] *See* HEW Report, *supra* note 156, at 6923-24 (proposing the Code of Fair Information Practices).

[163] REGAN, *supra* note 6, at 81. Although the final version of the Privacy Act of 1974 covered only federal agencies and did not create a separate agency to oversee all information practices

> [i]t gave individuals rights of access, correction, and knowledge about personal records in computerized or manual files; subjected federal agencies to standards of fair information handling; charged the Office of Management and Budget ("OMB") with responsibility for

information had been collected, for what purpose and to whom it had been released.[164] Although the Privacy Act exempted the Federal Bureau of Investigation ("FBI"), the Central Intelligence Agency and other protective agencies,[165] it provided statutory rights for citizens to begin to control their own personal information.

Three years later, in *Whalen v. Roe*[166] the Supreme Court, for the first time, recognized the right to informational privacy based on a zone of privacy that protected two kinds of interests: (1) avoiding disclosure of personal matters; and (2) independence in certain kinds of important decisions.[167] In upholding a New York statute requiring computer records of prescriptions to be filed with the state, the Supreme Court found that the filing, on its face, did not pose a sufficiently grievous threat to either interest so as to violate constitutional standards.[168] Thus, courts began to view personal information as existing within a protected sphere of some kind.

Previously, when data was part of the public record, courts used common-law principles to prevent consumers from complaining

---

implementation and oversight of the act; and established the Privacy Protection Study Commission to investigate the need for legislation over the private sector and the need for an oversight body over federal agencies.

REGAN, *supra* note 6, at 81-82.

[164] 5 U.S.C. § 552a(b). The Privacy Act of 1974 provided in part:

> [N]o [federal] agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with prior written consent of the individual to whom the record pertains.

Id.

[165] *Id.*

[166] 429 U.S. 589 (1977).

[167] *Id.* at 599-600 (characterizing "important decisions" as "matters relating to marriage, procreation, contraception, family relationships, and child rearing and education").

[168] *Id.* at 600. The Supreme Court in *Whalen v. Roe* considered the security of the database and the restrictions on the disclosure of information in its decision. *Id.*

about its distribution.[169] A recent Supreme Court case, however, held that disclosures of information compilations may invade privacy even when their component pieces are matters of public record.[170] Therefore, based on privacy laws and these common law decisions, the U.S. government began to be active in the area of personal privacy. The advent of the Internet and other networked communications mechanisms, however, has challenged the efficacy of such a piecemeal doctrine. New legislation attempts to address each TGI privacy issue as it arises.

C. *Communications Privacy and Consumer Empowerment Act*

Representative Edward Markey (D-Mass.) has introduced the Communications Privacy and Consumer Empowerment Act of 1996.[171] This proposed bill provides for the creation of Federal Communications Commission and Federal Trade Commission guidelines that would ensure privacy rights in communications, including on-line transactions.[172] As if to echo the findings of past committees, it proposes a Privacy Protection Committee and uses the Fair Information Code set forth in the HEW Report as the basis of a three-pronged model of disclosure that would provide consumers with: 1) knowledge—that personal information is being collected; 2) notice—that the recipient of the information intends to reuse, disclose or sell the information; and 3) a right to prohibit any such use.[173]

> New digital technologies and other innovations allow corporations to become more efficient workers, more

---

[169] Scott Shorr, Note, *Personal Information Contracts: How To Protect Privacy Without Violating the First Amendment,* 80 CORNELL L. REV. 1756, 1778 (1995).

[170] United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 780 (1989).

[171] H.R. 3685, 104th Cong., 2d Sess. (1996).

[172] *Id.* § 3-4.

[173] *Id.* § 3(a)(1)(A)-(C). "These Core rights are embodied in a proposal I have advocated for many years and I call it 'Knowledge, Notice and No.'" Markey Statement, *supra* note 1, at E1145-01.

> productive,[sic] and businesses to conduct commerce almost effortlessly in digital dollars. This same technology, however, will avail corporate America of the opportunity to track the clickstream of a citizen of the Net, to sneak corporate hands into a personal information 'cookie jar' and use this database to compile sophisticated, highly personal consumer profiles of people's hobbies, buying habits, financial information, health information, who they contact or converse with, when and for how long. In short, that wondrous wire may also allow digital desperadoes to roam the electronic frontier unchecked by any high technology sheriff or adherence to any code of electronic ethics.[174]

Although the bill is vague on whether its provisions will be required on an opt in or opt out basis, it clearly establishes the principles of control over one's personal information in the TGI context.

D. Consumer Internet Privacy Protection Act

Another pertinent bill was introduced on January 7, 1997, by Congressman Bruce Vento (D-Minn.). The Consumer Internet Privacy Protection Act of 1997 ("CIPPA")[175] would prohibit the disclosure of any "personally identifiable information"[176] by an interactive computer service[177] to any third party without the subscriber's informed written consent. CIPPA also requires such a service, upon the subscriber's request to: 1) provide the subscriber

---

[174] Markey Statement, *supra* note 1, at E1145-01. *See* Larry Jaffee, *Markey's Bill To Extend Online Privacy Protection to Consumers,* DIRECT MARKETING NEWS, July 8, 1996, at 3 (for a review of the newly introduced bill); *Bill Introduced To Protect Private Information on Internet,* TELECOMMUNICATIONS & NETWORK SECURITY REV., July 1996, *available in* LEXIS, News Library, Busdtl File (analyzing Markey's bill).

[175] H.R. 98, 105th Cong., 1st Sess. (1997).

[176] As defined by section 631 of the Communications Act of 1934 (47 U.S.C. § 551) (1934).

[177] Defined by the Consumer Internet Privacy Protection Act as "any information service that provides computer access to multiple users via modem to the Internet." H.R. 98, § 4.

with his or her personally identifiable information maintained by the service; 2) permit the subscriber to verify and to correct such information; and 3) provide the subscriber the identity of the third party recipients of such information.[178] The bill also grants the Federal Trade Commission investigative and enforcement authority[179] and provides for a private civil cause of action.[180] At the time of this writing, the bill had been sent to the Subcommittee on Telecommunications, Trade, and Consumer Protection. The legislation is a clear warning to Internet service providers and system administrators that even transactional information belongs to their customers and should be handled securely.

That the Consumer Internet Privacy Protection Act was proposed only several months after the introduction of the Communications Privacy and Consumer Empowerment Act is an illustration of two important dynamics. On the one hand, constituents, representatives and government officials are not content to wait for industry self-regulation when fundamental privacy violations are at stake. There is a general mistrust of informal industry standards and a motivation to put prophylactic protections in place. On the other hand, these two bills are a continuation of the historical pattern of industry-by-industry legislative response to technological threats to privacy. Although the bills directly address the privacy of TGI, albeit in two different contexts, they each are another in a long line of piecemeal attempts to protect against what is perceived as an isolated technological "threat" without articulating a more fundamental legal framework for deciding all future issues of personal privacy.

As examples of this "sectoral-specific" approach in the past two decades, laws in four areas, the cable/video, telecommunication, credit bureau and marketing industries, have tried to address privacy issues. In each case, private use of personal information has not been regulated to any substantial degree. More significantly, no fundamental principles of privacy have been codified in order to lay a groundwork for future confrontations between individuals'

---

[178] *Id.* § 2(c)(1).
[179] *Id.* § 3(a).
[180] *Id.* § 3(b)(2).

right of personal privacy and inevitable technological encroachments.

1. Cable/Video Regulation

In the 1980s two statutes were enacted that impose limitations directly on private parties to maintain consumer privacy in the video rental and cable television industries. First, the Video Privacy Protection Act of 1988 ("VPPA")[181] was enacted in response to the revelation, at the Supreme Court nomination hearings of Judge Bork, that a list of his video tape rentals had been procured and made publicly available.[182] VPPA prohibits video stores from giving third parties information about a customer's rentals or sales. However, mailing lists of customer addresses can be distributed under the VPPA.[183] An analogous bill, the Cable Communications Policy Act of 1984,[184] forbids cable operators and third parties from monitoring the viewing habits of subscribers.[185] Operators are required to inform subscribers of what personally identifiable information is collected and, the operators are generally barred from disclosure to third parties without consent.[186] However, the sale of cable operator's mailing lists is permitted when a subscriber has been given the opportunity to limit disclosure and such disclosure does not reveal the subscriber's viewing habits.[187] In this way, video rental stores can still sell their list of addresses and the cable industry is able to continue to exploit subscriber lists.

---

[181] 18 U.S.C. § 2710 (1988).

[182] *See* REGAN, *supra* note 6, at 199 (discussing other discrete events which led to the enactment of specific legislation).

[183] 18 U.S.C. §§ 2710-2711.

[184] 47 U.S.C. § 551 (1988).

[185] *Id.* § 551(c)(2)(C)(ii)(I).

[186] *Id.*

[187] *Id. See* Telecommunications Privacy Notice, *supra* note 11, at 6844 (describing the provisions of the Cable Communications Policy Act of 1984).

2. *Telecommunications*

The Electronic Communications Privacy Act of 1984 ("ECPA")[188] extended Title III protections[189] to the content of electronic communications including e-mail, cellular telephones, computerized transmission of data or video, and voice or display paging devices, but not to the collection of transmission profile data.[190] In fact, the ECPA even specifically allowed the electronic service provider to divulge transaction records to any government entity without judicial intervention.[191] The ECPA, because it pertained to any communication facilities that affected interstate or foreign commerce, did, however, eliminate the existing distinction between commercial and private carriers.[192] It is significant to also note that unlike its predecessor law, Title III, the ECPA enjoyed wide support from both private sector and government organizations.[193]

---

[188] 18 U.S.C. § 2510 (1986).

[189] Title III protects citizens against unauthorized government wiretaps. Pub. L. No. 90-351, 82 Stat. 213 (June 19, 1968) (codified at 18 U.S.C. §§ 2510-2520) (1968).

[190] 18 U.S.C. § 2510. Under the Electronic Communications Privacy Act of 1984 ("ECPA"), a provider of public telecommunications services cannot disclose the contents of an e-mail message without the consent of at least one of the parties. *Id.*; *see* 18 U.S.C. § 2511(3)(b). However, there is no specific restriction against the collection of personal information gathered from transaction data, nor is there a restriction on the duration of storage of such data. Reidenberg & Gamet-Pol, *supra* note 3, at 115.

[191] The entity must present at least an administrative, grand jury or trial subpoena. 18 U.S.C. § 2701(a).

[192] *Id.* § 2510(1).

[193] As Priscilla Regan points out, it took 40 years to pass Title III but only two years to reach an agreement on the ECPA. REGAN, *supra* note 6, at 135. Regan cites strong industry support as the most important reason. REGAN, *supra* note 6, at 135.

> Organizations that supported the final House bill represented all sectors of the communications and information industries, including the Electronic Mail Association, ADAPSO, the National Association of Broadcasters, the National Cable Television Association, the Videotext Industry Association, the Information Industry Association, the Direct

The Communications Assistance for Law Enforcement Act,[194] also know as the Digital Telephony Act ("DTA"), extended the ECPA's privacy protection to cordless telephones that lacked the traditional expectation of privacy.[195] DTA also addressed FBI concerns that communication service providers were previously not able to provide additional information to law enforcement officials about specific calls.[196] Therefore, DTA required "call setup information,"[197] or what the FBI termed "dialing information" to be provided when subpoenaed.[198] Although official access to such information was still limited by court monitoring, the DTA did not change the ECPA provision permitting non-regulated disclosure of the same information to "any non-government entity."[199]

The proposed Telephone Consumer Privacy Protection Act of 1993[200] would have regulated the use of Customer Proprietary Network Information ("CPNI") and Automatic Number Identification ("ANI") data.[201] It sought to ban all local exchange carriers from using CPNI: 1) to provide any service other than telephone service; 2) to identify or solicit potential customers for services

---

> Marketing Association, and the Associated Credit Bureaus . . . [t]his industry support is not surprising given the fact that . . . [the industry] realized that if they could not ensure privacy and security of their customers' communications, they would not be able to sell those products and services.

REGAN, *supra* note 6, at 135.

[194] Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C.A. §§ 1001-1010). Also known as the Digital Telephony Act.

[195] 47 U.S.C. § 1002(d).

[196] Freiwald, *supra* note 11, at 975-76.

[197] "Call setup information is defined as information generated which identifies the origin, destination and duration of the communication and includes codes punched in on a touch tone telephone, modem or fax tones, and e-mail address." Freiwald, *supra* note 11, at 978.

[198] 18 U.S.C. § 2703 (c)(1)(C) (1994).

[199] *Id.* § 2703(c)(1)(A).

[200] Telephone Consumer Privacy Protection Act of 1993, H.R. 3432, 103d Cong., 1st Sess. (1993).

[201] Customer Proprietary Network Information ("CPNI") and Automatic Number Identification ("ANI") are used in gathering Caller ID information and information about calls to "800" and "900" numbers. *See* Telecommunications Privacy Notice, *supra* note 11, at 6845-46.

other than telephone service; and 3) to provide customer equipment.[202] All ANI providers were prohibited from reusing or selling an identified number without notifying the calling party and providing an opportunity to limit or prohibit use.[203]

3. *Credit Bureaus*

The Fair Credit Reporting Act ("FCRA"),[204] the first information privacy legislation,[205] was amended by the Consumer Reporting Reform Act of 1994.[206] The FCRA attempted to address the concerns of the public about credit bureaus' misuse of personal information.[207] It required that credit reporting agencies use "reasonable measures" to protect the confidentiality of consumer information and ensure proper utilization of such data.[208] The law also conferred civil liability to any credit agency that is negligent or willful in its non-compliance with the FRCA.[209] Successful plaintiffs can, therefore, recover actual damages and reasonable attorney fees for negligence, and punitive damages for willful non-compliance.[210] In practice, however, loopholes and ambiguities in the law and First Amendment considerations have allowed credit bureaus to use and disclose consumer information almost at will.[211]

---

[202] Telephone Consumer Privacy Protection Act of 1993, H.R. 3432, 103d Cong., 1st Sess. tit. I, § 229(a).

[203] Consumer Privacy Protection Act of 1993, H.R. 3432, 103d Cong., 1st Sess. tit. II, § 230(b)(3).

[204] 15 U.S.C. § 1681 (1970).

[205] REGAN, *supra* note 6, at 101.

[206] 15 U.S.C. §§ 1681-1681(T) (1994) (as amended).

[207] *See generally* Prowda, *supra* note 74, at 752.

[208] 15 U.S.C. § 1681(b).

[209] *Id.* § 1681(n)-(o).

[210] *Id.*

[211] *See* Shorr, *supra* note 169, at 1791-93 (explaining that although the Fair Credit Reporting Act ("FCRA") requires credit bureaus to know the uses that third parties will make of a consumer's personal information, the act "barely limits" its subsequent use or resale by third parties).

4. *Direct Marketing*

In response to the increase in unsolicited advertising, especially the use of automatic dialing systems and commerce in mailing lists, twelve states had passed laws by 1991, banning automatic dialing, or at least limiting the hours it could be used.[212] The Telemarketing Protection Act of 1991[213] was passed to standardize such protections and expand them to unsolicited faxes.[214] *Destination Ventures, Ltd. v. Federal Communication Commission*[215] upheld the constitutionality of such restrictions on fax advertising.[216] Although the restriction on auto dialing was held unconstitutional in *Moser v. Federal Communication Commission*,[217] on appeal the limitations were found to meet constitutional standards.[218]

---

[212] *See, e.g.*, CAL. BUS. & PROF. CODE § 17563.5 (b) (Deering 1987); GA. CODE ANN. § 46-5-23(a) (1981); IOWA CODE § 476.57(2) (1991); KAN. STAT. ANN. § 50-670 (1991); LA. REV. STAT. ANN. § 45:811 (West 1991); MASS. ANN. LAWS ch. 159, § 19C (Law. Co-op. 1986); MINN. STAT. §§ 325E.28, 325E.30 (1987); MISS. CODE ANN. § 77-3-453 (1989); N.Y. GEN. BUS. LAW § 399-p(2) (McKinney 1988); OR. REV. STAT. § 759.290 (1989); TENN. CODE ANN. § 47-18-1502 (1990); WASH. REV. CODE § 80.36.400 (1986).

"No person may use an automatic dialing and announcing device for purposes of commercial solicitation. This section applies to all commercial solicitation intended to be received by telephone customers within the state." WASH. REV. CODE § 80.36.400(2). At least five states have passed laws since 1991 regulating such calls. *See, e.g.*, KY. REV. STAT. ANN. § 367.461 (Michie 1992); NEB. REV. STAT. ANN. § 86-1212 (1993); N.C. GEN. STAT. § 75-30 (1993); OHIO REV. CODE ANN. § 2917.21 (1996); VT. STAT. ANN. tit. 9, § 2511 (1992).

[213] 47 U.S.C. § 227 (1991)

[214] *Id.* § 227b(1)(C).

[215] 46 F.3d 54 (9th Cir. 1995) (holding that the ban on unsolicited fax advertising did not violate advertiser's First Amendment rights because the ban reasonably fit the government's interest in preventing shifting of advertising costs to consumers—in the form of paper, ink and telephone line time—and the ban was evenhanded as it applied to any organization).

[216] *Id.* at 56.

[217] 826 F. Supp. 360, 367 (D. Or. 1993), *rev'd*, 46 F.3d 970 (9th Cir.), *cert. denied*, 115 S. Ct. 2615 (1995).

[218] Moser v. Federal Communications Comm'n, 46 F.3d 970, 975 (9th Cir. 1994) (concluding that automated telemarketing calls are a threat to privacy that

IV. PRIVACY DOCTRINES

Although the underlying principles of both the Markey bill[219] and the Vento bill[220] are based on the Fair Information Code,[221] the enacted statutes cited in the preceding section have been largely reactive to privacy concerns and without any overarching privacy doctrine or the guidelines of an official privacy oversight body. As technology continues to present novel methods of intrusion into personal lives, privacy advocates seek legal grounding to support pro-active regulation against TGI dissemination. This Note provides analysis of two areas of law which may ultimately provide this basis—tort and property law.

A. Privacy Violation as Tort

Following the publication of Warren and Brandeis's influential article in 1890,[222] common law privacy developed independently in each state. In 1960, Dean Prosser identified four common law privacy torts[223] that were later adopted by the Restatement (Second) of Torts,[224] including: 1) publicity which unreasonably places the other in a false light before the public; 2) unreasonable intrusion upon seclusion of another; 3) unreasonable publicity given to the other's private life; and 4) misappropriation of the other's name or likeness.[225]

To establish a cause of action under the first category of false light publicity, the claimant must establish both that a falsity was communicated and that it became "public knowledge" in its

---

can be regulated, though not curtailed entirely, under the statute without violating the First Amendment), *cert. denied*, 115 S. Ct. 2615 (1995).

[219] H.R. 3685, 104th Cong., 2d Sess. (1996).

[220] H.R. 98, 105th Cong., 1st Sess. (1997).

[221] *See* HEW Report, *supra* note 156, at 6923-24.

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

[223] William Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

[224] RESTATEMENT (SECOND) OF TORTS § 652 (1977).

[225] *Id.*

communication to the public.[226] The second prong of this test—the communication of the information—appears applicable in the TGI context because personal data is compiled and disseminated to the public in a marketing database. However, the first prong—the veracity of personal transactional information—is not at issue because the data is recorded electronically and not subject to human error or falsification. Therefore, the tort of false light publicity would not generally be the basis for a viable TGI action.

The second tort, intrusion of seclusion, will also be problematic to apply in the TGI context. Intrusion of seclusion sets out three components that must be met to recover damages. The intrusion must be highly offensive to a reasonable person,[227] must be intentional[228] and must occur in a place where the plaintiff has a reasonable expectation of privacy.[229] It is difficult to say if this doctrine is applicable to TGI. Is the use of such information "highly offensive" or "outrageous"[230] rather than "merely offensive, insensitive, or intrusive?"[231] Cases have generally held that neither the solicitation nor the provision of information that is generally available "through normal avenues of investigation, inquiry or observation" are *per se* not highly offensive.[232]

---

[226] DAVID A. ELDER, THE LAW OF PRIVACY §§ 4:2-:4, at 274-99 (1991).

[227] RESTATEMENT *supra* note 224, § 652B.

[228] RESTATEMENT *supra* note 224, § 652B & cmt. a.

[229] RESTATEMENT *supra* note 224, § 652B & cmt. b.

[230] RESTATEMENT *supra* note 224, § 652B & cmt. d.

[231] *See, e.g.*, Seaphus v. Lilly, 691 F. Supp. 127, 132 (N.D. Ill. 1988) (obtaining unlisted phone number found not to be tortious); N.O.C., Inc. v. Schaefer, 484 A.2d 729, 733 (N.J. Super. Ct. 1984) (finding mild surveillance of suspected illegal dumping not tortious); Chicarella v. Passant, 494 A.2d 1109, 1114 (Pa. Super. 1985) (ruling solicitation by deception or disclosure of confidential medical information that is not particularly embarrassing not sufficiently offensive).

[232] ELDER, *supra* note 226, § 2:1, at 21 (1991 & Supp. Mar. 1996). *See, e.g.*, Wolf v. Regardie, 553 A.2d 1213, 1218, (D.C. Ct. App. 1989) (holding that garnering information from third parties and public records about plaintiff's business deals are matters of public record or "knowledge readily available to anyone who would wish to obtain it" and therefore does not constitute intrusion); Dwyer v. American Express Co., 652 N.E.2d 1351, 1354-55 (Ill. App. Ct. 1995) (rejecting intrusion claim for defendant's renting of information regarding credit cardmember's spending propensities used by recipients for targeted marketing).

Although the "taking" of transactional information clearly seems intentional, one defense to this element could be that the information was not obtained by an actual intrusion, but was gathered passively.[233] Furthermore, it is doubtful that Internet use carries a reasonable expectation of privacy, and this element would, therefore, not be met. Finally, who is doing the "intruding" will impact on the weighing of factors. For example, an Internet service provider might be able to use personal information under the theory of an implied privilege.[234]

The third privacy tort, that of public disclosure of private facts, also fails to provide a sure remedy against TGI use. Most transactional information disclosures do not satisfy the three elements necessary to fall within this doctrine. These elements are that the disclosure must be found "highly offensive,"[235] the plaintiff must be "reasonably identifiable from the matter disclosed"[236] and the information must reach so many people that it becomes "public knowledge."[237] As in the intrusion tort, whether use of TGI meets the highly offensive standard is questionable. Although a "reasonable" identification can be made of a user from his or her TGI it is not a particular plaintiff but rather a particular computer that is being identified.[238] Again, the public knowledge requirement will easily be met when TGI is distributed for use on-line. Hence, the net result here is that the tort of disclosure of private facts will also have trouble providing protection from unauthorized use of TGI.

---

[233] *See* Pearson v. Dodd, 410 F.2d 701, 705 (D.C. Cir.) (holding that the news media's passive receipt of information regarding a senator was not tortious), *cert. denied*, 395 U.S. 947 (1969).

[234] How courts have treated credit bureaus' use of private information is illustrative of how they might view intrusions into TGI. Credit bureaus have established a qualified privilege to disseminate credit reports. Shorr, *supra* note 169, at 1778. This has rested on the grounds that such information is an "integral part of the business community," is available via "normal avenues of investigation, inquiry or observation" and that consent for such activities is implicitly given to the credit card company, stores that honor the card and credit bureaus themselves when the credit application is signed. Shorr, *supra* note 169, at 1778.

[235] RESTATEMENT, *supra* note 224, § 652D.

[236] ELDER, *supra* note 226, § 3:3B, at 162.

[237] RESTATEMENT, *supra* note 224, § 652D cmt. a.

[238] *See* CDT Privacy Page, *supra* note 30.

However, there is one tort, the fourth tort, that seems to specifically address the harm of TGI: misappropriation. Although applied more often to well-known personalities,[239] the tort of misappropriation implies a deprivation of dignity and economic loss to any person.[240] It is the non-consensual use of one's name or likeness for the economic or other benefit of the appropriator.[241] Furthermore, to meet this standard it must be shown that the plaintiff's name or likeness was appropriated for the defendant's advantage.[242] Because TGI can be seen as a "personality profile" analogous to a person's image,[243] and, in marketing contexts, it is clearly of economic advantage, it would appear that the non-consensual use of on-line transaction information satisfies these factors,[244] and would produce a sustainable argument for misappropriation.

In sum, the original four privacy torts provide tenuous protection against the use of TGI. One author has argued for a new tort—tortious commercial dissemination of private facts—which is based on an "undifferentiated interest in human dignity" and protects the same values protected by the four Prosser torts.[245]

---

[239] *See* Onassis v. Christian Dior-N.Y., Inc., 122 Misc. 2d 603, 472 N.Y.S.2d 254 (Sup. Ct. 1984), *aff'd*, 110 A.D.2d 1095, 448 N.Y.S.2d 943 (1st Dep't 1985) (mem.).

[240] ELDER, *supra* note 226, § 6:1, at 379.

[241] ELDER, *supra* note 226, § 6:2, at 380.

[242] ELDER, *supra* note 226, § 6:2, at 380.

[243] Jonathan P. Graham, Note, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395, 1413 (1987).

[244] It should be noted that courts have been reluctant to impose penalties on defendants who sell consumer lists for advertising purposes. *See* Shibley v. Time, Inc., 341 N.E.2d 337, 340 (Ohio Ct. App. 1975) (selling of subscription lists to direct marketers did not constitute an invasion of privacy); Joel E. Smith, Annotation, *Invasion of Privacy by Sale or Rental of List of Customers, Subscribers, or the Like to One Who Will Use It for Advertising Purposes*, 82 A.L.R.3d 772 (1978).

[245] Graham, *supra* note 243, at 1419, 1428. Graham's "tortious commercial dissemination of private facts" recognizes the uses that can be made of personal information in electronic communication. Graham, *supra* note 243, at 1412. "Clearly the traditional definitions of what constitutes a privacy tort do not encompass the problem of information privacy because the cases that led to their development were decided before new information techniques became prevalent."

Despite the hurdles to creating a new cause of action, as well as the apparent reluctance of courts to restrict commercial activities,[246] the new tort of tortious commercial dissemination of private facts is one viable foundation for the expansion of privacy protection in the digital age. In the alternative, this Note argues for at least the application of the misappropriation tort when personal information is used without consent and to the detriment of the consumer.

B. Privacy as Property Right

Another traditional area of law that might successfully be applied to the unauthorized dissemination of personal information and TGI is property law.[247] In reality, property law was one of the doctrines underlying Warren and Brandeis's establishment of a

---

Graham, *supra* note 243, at 1418. Graham sets out several levels of conduct that could be encompassed by this new cause of action. First, he questions at what level information gathering should be controlled, and decides that it should be controlled at the point dissemination is attempted. Next, he concedes that not all information collection is harmful but would allow the common law to draw distinctions between notorious and benign uses. Finally, the restrictions must pass constitutional muster in the face of First Amendment arguments. Graham proposes a judicial balancing of interests similar to the test used in *New York Times v. Sullivan*, 376 U.S. 254 (1964). He further argues that correctly weighing the interests of commercial non-press speech would enable such a remedy to meet First Amendment standards and be held constitutional. *See* Graham, *supra* note 243, at 1428-38.

[246] *See supra* note 244 (discussing cases in which commercial uses of information have been allowed).

[247] *See generally* Arthur R. Miller, *Personal Privacy in the Computer Age: The Challenge of New Technology in an Information-Oriented Society*, 67 MICH. L. REV. 1091, 1223-26 (1969) (discussing the granting of a property right in personal information).

> Perhaps the most facile approach to safeguarding privacy is the suggestion that control over personal information be considered a property right, vested in the subject of the data and eligible for the full range of constitutional and legal protections that attach to property.

Id. at 1223-25. *See* ALAN WESTIN, PRIVACY AND FREEDOM 324-25 (1967) (calling for defining the right of decision over "private personalty" as a property right with all the attendant due process guarantees and regulation).

privacy tort.[248] They drew on common law copyright principles to support the premise that there is a property right in "personal interest" such as the right to be let alone.[249] In particular, intellectual property interests in trade secret protection and the right of publicity seem applicable to the sale of TGI personal information to direct marketers.

A trade secret has value because it is private and therefore restrictions can be placed on a third party's use. Trade secrets represent "the right to retain exclusive control or knowledge of certain information."[250] In addition, trade secrets must meet the following criteria to be protected in court:

(1) few outside the claimant's business know the information;
(2) the claimant has limited disclosure of the information within his business;
(3) the claimant has taken reasonable precautions to ensure the secrecy of the information;
(4) the information is valuable to the claimant and gives him a competitive business advantage;
(5) the claimant had developed or acquired the information at some expense; and
(6) the information is difficult to acquire from other sources.[251]

It is arguable that if an individual's use of his or her computer to obtain information from networks is considered his or her

---

[248] Warren & Brandeis, *supra* note 222, at 200.

[249] Diane L. Zimmerman, *Information as Speech, Information as Goods: Some Thoughts on Marketplaces and the Bill of Rights,* 33 WM. & MARY L. REV. 665, 699 (1992). Interestingly, the tort was predicated on the general principle of an "inviolate personality" that also underlies copyright and other intellectual property rights. Warren & Brandeis, *supra* note 222, at 205-06.

[250] RAYMOND T. NIMMER, THE LAW OF COMPUTER TECHNOLOGY 16.02 (2d ed. 1992).

[251] RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939). *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 (1995) (discussing the modernized standard on trade secrets).

"business," then TGI personal information substantially meets these criteria and could be protected as a trade secret.

It is also possible that the privacy of our TGI personal information is a property right much like the right of publicity granted to celebrities. Under this common law doctrine, a plaintiff, usually a famous individual, has a cause of action to recover damages for any economic harm to the value of the plaintiff's identity.[252] A defendant's liability is based on the use of the celebrity's name or physical likeness for the defendant's own pecuniary benefit without the individual's consent.[253] It is now well established that this right extends to non-celebrities as well.[254] "If one's identity has commercial value, one should have a right to control and benefit from its commercial uses, regardless of whether one is a celebrity."[255] As with all property, the right of publicity can be assigned and licensed.[256] In the TGI context, the recognition of a right of publicity in one's personal information confers property status on this information that can then be protected and exploited by the computer user.[257]

---

[252] THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 3.1[B], at 3-3 (1994). A right of privacy plaintiff must prove: (1) ownership of an enforceable right in his or her identity; (2) that the defendant (a) used some aspect of the plaintiff's identity or persona, (b) without the plaintiff's consent and (c) in a manner that rendered the plaintiff identifiable; and (3) that the defendant's use is likely to damage the commercial value of the plaintiff's identity. *Id.*

[253] *Id.*

[254] *See* Motschenbacher v. R.J. Reynolds Tobacco Co., 498 F.2d 821, 824 n.11 (9th Cir. 1974). *See also* Tellado v. Time-Life Books, 643 F. Supp. 904, 913 (D.N.J. 1986) (finding a right for a non-celebrity to be compensated for the use of his or her likeness); Onassis v. Christian Dior-N.Y., Inc., 122 Misc. 2d 603, 610, 472 N.Y.S.2d 254, 260 (Sup. Ct. 1984) (reviewing interpretation of state privacy statute and concluding that "all persons, of whatever station in life, from the relatively unknown to the world famous, are to be secured against rapacious commercial exploitation"). *See generally* ELDER, *supra* note 226, § 6.1, at 379; MCCARTHY, *supra* note 252, § 4.3.

[255] Shorr, *supra* note 169, at 1827.

[256] ELDER, *supra* note 226, § 6.1, at 377 n.8; MCCARTHY, *supra* note 252, § 10.3[B][1].

[257] Under this argument, because all individuals have the power to hypothecate their property, personal data can be exploited via contract or license.

Trade secrets and the right of publicity are two areas of property law that could be reasonably applied to control unauthorized uses of personal information taken from the Internet and other communication networks. When combined with the legitimization of tortious claims for the same harms, a basis for privacy protection is established that is far sturdier than the fencing erected over the past thirty years by the individual laws discussed above.

Based on deeply rooted principles in common law and property rights, such a conceptualization avoids the familiar political struggle to set a negotiated standard for privacy rights. The property and tort approaches acknowledge the fundamental nature of personal privacy. They institute the same kind of protections and accountabilities proposed by privacy advocates when they unsuccessfully fought for a privacy bureau and a code of privacy principles. Although the two proposed bills attempt to put in place the same ideas, they are once again a reaction to specific threats in circumscribed industries. The larger doctrinal change, on the other hand, establishes a bulwark likely to withstand the ravages of technology leaps and policy swings and therefore maintain personal autonomy over our individual TGI—a powerful and valuable new commodity.

CONCLUSION

The commercial use of transaction generated personal information in networked computer environments represents the latest and most significant challenge to personal privacy in the United States. In the past, new technologies also posed dangers to personal privacy and were addressed in turn, culminating in sector-specific regulation. Whenever technology has enabled commercial interests

---

"If there is value in it, sufficient to excite the cupidity of another, why is it not the property of him who gives it the value and from whom the value springs?" ELDER, *supra* note 226, § 6:1, at 376 (quoting Munden v. Harris, 134 S.W. 1076 (Mo. 1911)). "[A] federal statute focused on the proprietary origins of privacy could improve substantially upon current law by recognizing property rights in personal information and enabling personal information contracts to govern major informational transactions." Shorr, *supra* note 169, at 1818. Without a federal statute, common law will not be able to provide standardized nationwide protection. Shorr, *supra* note 169, at 1818 n.301.

to intrude upon individual privacy, legislation has been promulgated to prevent abuses in each industry. Despite the protections of the First Amendment and the promise of self-regulation, industry has been statutorily bridled against its natural competitive and commercial tendencies to use information to the particular industry's best advantage. In each instance, similar issues were presented: lack of personal control, information gathered for one purpose used for another, surplus information stored and errors not addressed and inter-organization usage. Strong cases were made for consumer control of personal information, enforcement agency oversight and guidelines for commercial uses. However, the strength of the commercial lobby succeeded in restricting the scope of each problem to its unique issues, thereby creating only narrow legislation.[258]

It is, therefore, evident that official statutory protection is essential to control intrusions into computer TGI privacy. The proposed Communications Privacy and Consumer Empowerment Act of 1996[259] and the proposed Consumer Internet Privacy Protection Act of 1997[260] offer such protections and should be passed as soon as possible.

Furthermore, the power and interconnectivity of the digital network and its growing ubiquity in our society present a challenge wholly different from past threats to privacy. The unprecedented nature of this challenge calls for new legislation and something more: a substantive expansion of legal privacy protection doctrine to include tort and property rights in order to guard against the non-consensual use of TGI. These two legal theories may also provide a broadened legal basis to protect individuals' privacy from technologies not yet developed.

---

[258] For examples of narrowly drawn legislation see the Fair Credit Reporting Act, the Cable Communications Policy Act, the Video Privacy Protection Act and the Telemarketing Protections Act. *See supra* Part III.C.1-4 (discussing existing legislation).

[259] Communications Privacy and Consumer Empowerment Act of 1996, H.R. 3685, 104th Cong., 2d Sess. (1996).

[260] Consumer Internet Privacy Protection Act, H.R. 98, 105th Cong., 1st Sess. (1997).

Although the issues in each past technological challenge are similar to the TGI issues we now face—intrusion into private activities—the enormity of the qualitative and quantitative intrusion puts TGI into a different category altogether. At the dawn of a new "networked" age that will link individuals into a "global community," there is a tremendous risk of losing control over easily obtained, personal and essential information—information that contributes to our "inviolate personality."[261] In the future of networked communication, not only will networks extend into communities and create links to providers of shopping, education, social and financial services, but networks will extend "inward" and links with domestic "personal services" will be ubiquitous.[262] If strong personal privacy protections are not put in place today, access to TGI from such internal networks will allow commercial entities access to much more than mere mailing lists.

---

[261] Warren & Brandeis, *supra* note 222, at 205-06.

[262] Tiny processors may link your "command center" (on your watch or personal communicator, perhaps) with information monitoring and control capabilities for appliances, computers, vehicle maintenance, home temperature and security control. David Kline, *The Embedded Internet,* WIRED, Oct. 1996, at 98.