『서울대학교 法學』 제51권 제4호 2010년 12월 229～268면
Seoul Law Journal Vol. 51 No. 4 December 2010. pp. 229～268

〈논문〉

The Difficulties Current American Law Faces in Protecting Internet Users' Privacy : The Devil is in the Details*

Lydia Kang**

Abstract

This article provides an analysis of the laws potentially applicable to the online collection and use of personal information by the private sector. It begins by examining corporations' current practices of deploying sophisticated software to gather, use, and disclose information about users. The article contends that current applicable law, particularly federal statutory law, is too fragmented and dated to properly safeguard individuals' privacy rights on the Internet. The article proceeds to define the privacy interests at stake and considers and ultimately rejects the arguments that many users either do not care that their online behavior is tracked and their data mined or that they give companies fully informed consent related to the data collection. Finally, the article offers a brief proposal for a comprehensive federal statute regulating the use and security of personal information in the hands of companies.

Key words: Personally identifiable information, cookies, beacons, behavioral tracking, data broker, omnibus federal legislation, Electronic Communications Privacy Act

* 이 연구는 2010년도 서강대학교 교내연구비 지원에 의한 연구임(201010014.01).

** Assistant Professor of Law, Sogang Law School. Special thanks to Sunyoung Baek for her helpful research.

Lately, hearing about a company's publicity snafu regarding privacy has become almost a regular occurrence. Such news has helped some in the general public to realize that information about what websites they visit, links they click, and searches they conduct on the Internet is being collected by commercial entities. However, the level of detail gathered and the power of the tools deployed are not known. Moreover, many users are unaware of the myriad potential uses of the data. Nor do most people know what security measures, if any, are in place to protect their information from misuse. Given the risks posed by this capture of data, there has been a push for federal legislation[1] regulating privacy in the private sector. At the same time, companies and other interests have argued that the current regulatory regime, albeit consisting of piecemeal legislation and self-regulation, is sufficient. This paper aims to address the question of whether more federal legislation is necessary in the current environment.

The article proceeds in the following parts : Part I briefly gives an overview of the law related to privacy, particularly focusing on the law that relate to commercial entities. It highlights the fragmented nature of current federal legislation and the weaknesses of self-regulation. Part II discusses the meaning and value of privacy (influenced by the pragmatic approach of Daniel J. Solove)[2] in the context of current practices on the Internet (in which companies gather data and compile detailed dossiers on users). This part discusses how such practices disrupt individuals' privacy interests and expectations in three ways, largely due to the implications of collecting and bartering so much detail about users. Part III discusses whether, due to the potential privacy harms, there should be omnibus federal legislation.[3] It considers the argument that users willingly give up information about themselves in exchange for access to the free information and services companies offer. Ultimately, the

---

1) This paper focuses on American privacy law. Although there are similarities in the protections of information privacy across jurisdictions, United States privacy law is relatively atypical in that unlike,e.g., European law, the relevant federal statutes in America are sectoral, applying to specific industries or problems.

2) Daniel J. Solove, *Conceptualizing Privacy*, 90 Cal .L. Rev. 1087 (2002).

3) Omnibus federal legislation would consist of a comprehensive statute regulating the private sector's collection, use, and disclosure of personal information.

analysis concludes that it is unlikely most users are fully aware of the scope of data being collected, what the uses could be, and, perhaps most importantly, how the disparate details can be pieced together to the point of identifying them. It also suggests that we are confronted with a simmering problem reminiscent of the financial products disaster. In the years leading up to the 2008 economic meltdown, United States government agencies appeared reluctant to regulate financial products, reasoning that, despite the power imbalance between consumers and the financial institutions selling credit products, consumers were fully informed when they signed up to purchase. Just as this assumption was debunked by the financial crisis, the argument that Internet users make fully informed decisions to give up their data when they visit company websites is questionable at best. Part IV concludes with a modest proposal for federal legislation that would better protect the privacy interests of Internet users.

I. A Weak Legal Framework

The Internet currently reaches about 77.3 percent of the United States population.[4] For many, the Internet has opened new means of communication and access to free content and services. At the same time, unbeknownst to some users, their online behavior, including every website they visit, could be subject to monitoring and tracking. Currently, companies can legally collect information about consumers using a variety of technological tools. This information includes what searches they make, what they purchase, what medications they order, and what their credit history is. An individual's location, literary and music interests, habits, and relationships are up for grabs. For example, there are companies today that can identify someone on the Internet as a woman in her thirties, who is married, has several children, and rents comedies, shops at Target, listens to country music, and resides in Colorado Springs. Computer software can organize this data and prepare it to be sold, shared, and used

---

4) Internet World Stats, Usage and Population Statistics, http://www.internetworldstats.com/am/us.htm (last visited Nov. 14 2010).

by direct marketing companies, lending institutions, insurance companies, and credit bureaus. The online profile is then used to launch more targeted and therefore more lucrative advertising.

This trading in personal information has been capitalized on by commercial entities for some time.[5] However, the minutiae of data gleaned, the speed with which it is shared, and the nature of the tools used have all rapidly advanced in recent years. Online marketing used to mean that advertisers bought advertisements on specific web pages a toy advertisement on a toy website for example. Now, however, advertisers pay to follow people around the Internet with highly targeted messages. This type of consumer tracking underpins an online advertising economy that racked up $23 billion in ad spending last year. Behavior tracking is everywhere now. Researchers at AT&T Labs and Worcester Polytechnic Institute discovered tracking technology on 80% of 1,000 popular websites, as compared to 40% of those sites in 2005.[6]

Not only has the monitoring increased, the software technology deployed has become ever more sophisticated. Surveillance tools can collect information about users and track behavior so rapidly that a profile of the user can be auctioned off in real time to the highest bidder who can then show the user a targeted advertisement within seconds. The tools include “cookies,”[7] which can build detailed dossiers on

---

5) Many of the largest Internet companies have significant stakes in online advertising. Google bought DoubleClick, an online advertising company, on April 14, 2007 for 3.1 billion. The deal was motivated by Google’s interest in behavioral advertising, in which companies use information collection techniques to follow users around the Internet and show them targeted ads. Louise Story and Miguel Helft, *Google Buys DoubleClick for $3.1 Billion*, The New York Times, April 14, 2007. See also Julia Angwin, *The Web’s New Gold Mine: Your Secrets*, The Wall Street Journal, July 30, 2010 (“Microsoft bought aQuantive, a Web-ad firm, in 2007 for morethan $6 billion, to build a business selling ads online. Google, already a giant in online marketing, in September 2008 launched a Web browser, Chrome, that gives it new insight into Internet users’ habits. Apple has launched an ad network, iAds, for its iPhone and iPad. And Adobe last year paid $1.8 billion to buy Omniture, which measures the effectiveness of online ads.”) The buying spree for online advertising business continued into this year. After Google purchased AdMob, a mobile advertising network, for $750 million last November, Apple acquired Quattro Wireless, a mobile advertising company, early this year. http://dealbook.nytimes.com/2010/01/06/apple-buys-quattro-an-ad-firm/

6) Angwin, supra.

individuals and “deep-packet inspection,”[8] a tool that gives companies the ability to track every website users visit and provides a detailed look at everything they’re doing, such as where they’re going on vacation, who is traveling with them, how much they spend on the trip and what credit card was used. In addition, software called a “beacon” can capture what people are typing on any given website - and thereby learn their curiosities, thoughts, and concerns.[9]

A recent study revealed the startling number of surveillance tools found on America’s most popular 50 websites.[10] The study concluded that the country’s top 50 websites on average installed 64 pieces of tracking technology onto personal computers, usually with no warning. Twelve sites each installed more than a hundred. The study further discovered that tracking technology has become more clever and surreptitious. For example, tracking of user’s behavior used to be done mostly by cookie files that record websites visited. However, newer tools scan in real time everything a person does on a website, and then instantly access the visitor’s location, interests, and even health condition.[11] Even if a user tries to delete or block the surveillance tools, some can simply re-spawn themselves.

The law has remained largely silent regarding tracking technology. American courts have ruled that it is legal for companies to use the most basic tracking tool,

---

7) Cookies are bits of encrypted information deposited on a computer’s hard drive by websites it has accessed, and which store details of the user’s activity on that site. This enables the site’s server to recognize the computer the next time it visits, so that the user will be provided with the same layout, shopping cart, search information, personalized greetings and settings. Some cookies track the activities of the user from website to website. For example, whenever a user is logged in to Facebook and surfing the web, she is also transmitting information about the websites she’s visited to Facebook. Ryan Singel, Today Facebook, *Tomorrow the World*, Wired, Apr. 23, 2010, available at http://www.wired.com/ epicenter/2010/04/ facebook-becomes-web/comment-page-1.

8) Plaintiffs filed a class action lawsuit regarding behavioral advertising against NebuAd Inc., an online advertising company last year. Plaintiffs accuse the company of spying on consumers from several states andviolating their privacy and computer security rights. The lawsuit specifically alleges that NebuAd conducted deep-packet inspection. *Valentine v. NebuAd*, No. 08 Civ. 5113 (N.D. Cal. Nov. 10, 2008).

9) Angwin, supra.

10) Id.

11) These profiles of individuals are bought or sold on exchanges.

cookies; however, they have not thus far ruled on the more invasive trackers. Companies therefore feel largely free, within parameters outlined below, to follow us around creating digital dossiers, which "are not controlled by us but by various entities, such as private-sector companies..."[12] American privacy law has not fully wrested control back to the consumers.

Privacy law is the area of law concerned with the protection and preservation of the privacy rights of individuals. Increasingly, governments and other public as well as private organizations collect enormous amounts of personal data about individuals for a variety of purposes. The law of privacy regulates the type of information which may be collected and how this information may be used.

While there is a hodgepodge of American laws (e.g., constitutional, statutory, common law) relating to privacy, this article will, for the sake of clarity, focus on the specific law and regulations pertaining to the private sector.[13] Several federal statutes are potentially applicable to the collection and use of personal information by commercial entities. These statutes are generally sector specific, meaning that they are narrowly tailored to specific types of business or types of problem. For example, there are federal statutes regulating the gathering, use and disclosure of information related to personal health,[14] children,[15] entertainment records,[16] and

---

12) Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 Hastings L.J. 1227, 1251 (2003).

13) Banks, financial institutions, insurance companies, credit reporting agencies are not included in this analysis. These entities are covered under separate federal legislation.

14) Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.). The privacy regulations are codified at 45 C.F.R. pts. 160, 164 (2008 & Supp. 2009).

15) 15 U.S.C. §§ 6501-6508; 16 C.F.R. Part 312. Children's Online Privacy Protection Act (1998): Congress passed the Children's Online Privacy Protection Act (COPPA) to protect children's personal information from its collection and misuse by commercial web sites. On October 20, 1999, the FTC issued a Final Rule implementing the Act, which went into effect on April 21, 2000. COPPA requires Web sites and other online services directed at children under 13, or which collect information regarding users' age, to provide parents with notice of their information practices and obtain parental consent prior to the collection of personal information from children. The Act further requires such sites to provide parents with the ability to review and correct information about their children collected by such services. The Commission has expressed concern that this Act may already be outdated in that it does not necessarily apply to online gaming sites or mobile applications.

internet use and electronic communications.[17]

Among these federal statutes, the two that plaintiffs have tried to use the most to prevent the collection of personal data by companies are the Electronic Communications Privacy Act ("ECPA") and the Computer Fraud and Abuse Act ("CFAA"). These efforts have been largely unsuccessful. In one case, plaintiffs in In re DoubleClick Inc. Privacy Litigation,[18] argued that DoubleClick's use of cookies to track an individual and build a profile of the person violated the ECPA. Title I of the ECPA (The Wiretap Act) provides that any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept, any ··· electronic communication" shall be punished or subject to lawsuit. However, the statute provides for an exception to this liability if one of the parties to the communications "has given prior consent to such interception···[19] The Court agreed with DoubleClick's argument that the consent exception applied since one party to the communication (the websites using

---

16) Videotape Privacy Protection Act of 1988, as codified at 18 U.S.C. §2710; see also The Cable Communications Policy Act, as codified at 47 U.S.C. §551(a)(1).

17) Electronic Communications Privacy Act, as codified at 18 U.S.C. §2510; Computer Fraud and Abuse Act, as codified at 18 U.S.C. §1030. Unsolicited call, facsimiles, and email (spam) for advertising/marketing purposes are regulated by Telephone Consumer Protections Act, 47 U.S.C. §227 ("TCPA") and CAN-SPAM Act, 15 U.S.C. §§7701. Mobile marketing is limited particularly by TCPA and CAN-SPAMAct. If a text message is sent by referencing a domain name (sent to a consumer's cell phone through the consumer's mobile service provider e-mail gateway), the text is subject to CAN-SPAM. Under TCPA, companies cannot send texts using an automatic telephone dialing system unless the recipient has given his or her prior express consent. Companies are also prohibited from initiating a telephone solicitation − i.e., a call made for the purpose of encouraging the purchase of goods or services − to a number listed on the do-not-call registry without either having (a) the recipient's prior express invitation or (b) an established business relationship with the recipient. In addition, a company cannot send a telemarketing message (a message to encourage the purchase of a product or service) if it does not have in place measures for creating its own opt-out list. Even if an automatic telephone dialing system is not used, if the message is a solicitation, other parts of TCPA must be followed. In particular, the company still (a) may only send the message between 8 am and 9 pm and must maintain a process for obtaining and recording any opt out requests it receives, or (b) must have obtained the recipient's express consent or have a prior business relationship with the recipient.

18) 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

19) 18 U.S.C. 2511(2)(d).

DoubleClick) had consented. Consent precludes a claim under the Wiretap Act. In other cases, courts have considered plaintiff's claims that companies' surveillance tools violated Title II of the ECPA (Stored Wire and Electronic Communications and Transactional Records Act). Title II of the ECPA prohibits a person or entity from (1) intentionally access[ing] without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage.[20] However, court has held that since companies selling traditional products and services online are not providing an "electronic communication service," they fall outside the scope of the statute.[21] In another case involving Title II of the ECPA, plaintiffs sued several pharmaceutical corporations who had hired a third party to monitor their companies' websites and provide analysis of website traffic. The monitoring, according to plaintiffs, entailed collecting personal information, including health information and web browsing habits, without users' knowledge or consent. The tracking was done by cookies and other devices. Plaintiffs alleged here that the ECPA prohibited this surveillance. The court ruled in favor of defendants, reasoning that an individual plaintiff's personal computer is not a "facility through which an electronic communication service is provided."[22]

---

20) 18 U.S.C. §2701(a).

21) See, e.g., *Dyer v. Northwest Airlines Corp*., 334 F.Supp.2d 1196 (D.N.D. 2004).

22) *In re Pharmatrak, Inc. Privacy Litigation*, 220 F.Supp.2d 4, 13 (D.Mass. 2002). The court noted "Plaintiffs find it noteworthy that '[p]ersonal computers provide consumers with the opportunity to access the Internet and send or receive electronic communications,' and that '[w]ithout personal computers, most consumers would not be able to access the Internet or electronic communications.' Fair enough, but without a telephone, most consumers would not be able to access telephone lines, and without televisions, most consumers would not be able to access cable television. Just as telephones and televisions are necessary devices by which consumers access particular services, personal computers are necessary devices by which consumers connect to the Internet. While it is possible for modern computers to perform server-like functions, there is no evidence that any of the Plaintiffs used their computers in this way. While computers and telephones certainly provide services in the general sense of the word, that is not enough for the purposes of the ECPA. The relevant service is Internet access, and the service is provided through ISPs or other servers, not though Plaintiffs' PCs."

Plaintiffs have also tried to claim that the collection and use of personal data by companies violate provisions of the Computer Fraud and Abuse Act ("CFAA"),[23] but have confronted difficulty in demonstrating sufficient damages under the statute to prevail in court. The courts have held that individual plaintiffs cannot add up their damages to meet the statutory requirement of suffering at least $5,000 in damages. Damages could only be combined "for a single act" against "a particular computer."[24] Since plaintiffs only alleged that multiple acts had been made against different computers, they could not succeed under CFAA.

While private lawsuits have not met with significant success, the Federal Trade Commission ("FTC") has become gradually more active in enforcing, at a minimum, that companies adhere to explicit promises they make regarding privacy on their websites. The Federal Trade Commission Act ("FTC Act") empowers and directs the FTC to investigate business practices, including data collection practices that constitute consumer harm.[25] Specifically, the FTC determines, on a case by case basis, whether or not to open an investigation against a companyaccused of violating Section 5 of the FTC Act, relating to business practices that constitute unfair[26] and deceptive[27]

---

23) The CFAA provides imposes liability on "[w]hoever knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period."

24) See, e.g., *In re Pharmatrak, Inc. v. Privacy Litigation*, 220 F.Supp.2d 4 (D.Mass. 2002) and *In re Doubleclick Inc. Privacy Litigation*, 154 F.Supp.2d 497 (S.D.N.Y. 2001). This requirement of proving damages has also stymied some plaintiffs' efforts to sue companies on breach of contract grounds. See, e.g., *In re Northwest Airlines Privacy Litigation*, 2004 WL 1278459 (D. Minn. 2004).

25) 15 U.S.C. § 45.

26) A trade practice is unfair or deceptive if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C.§ 45(n); see, e.g., *Fed. Trade Comm'n v. Seismic Entertainment Productions, Inc.*, Civ. No. 1:04-CV-00377 (Nov. 21, 2006) (finding that unauthorized changes to users' computers that affected the functionality of the computers as a result of Seismic's anti-spyware software constituted a "substantial injury without countervailing benefits.").

27) The FTC will make a finding of deception if there has been a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances,

trade practices.[28] Under the Act, the FTC may commence civil actions for penalties for a knowing violation of the Act[29] as well as seek injunctive relief.[30] The Act does not provide for private causes of action.

The Commission has indicated that it views its work as promoting the fair information practices of notice, choice, access, and security.[31] Its privacy agenda has focused primarily on the following areas : (1) data security enforcement; (2) identity theft;[32] (3) children's privacy; and (4) protecting consumers from spam, spyware, and telemarketing.[33] Since 1998, the FTC has made clear that failure to adhere to stated privacy policy or the use and disclosure of personal information in a manner inconsistent with a posted policy is a deceptive practice under the FTC Act.[34] The FTC also has carried out enforcement actions against companies that fail to take reasonable measures to protect customer data or misrepresent their data security policies.[35] In a typical data security complaint, the FTC alleges that the company's

---

to the consumer's detriment. Fed. Trade Comm'n, FTC Policy Statement on Deception (1983), available at http://www.ftc.gov/bcp/policystmt/ad-decept.htm.

28) The FTC does not have jurisdiction over specific types of companies such as financial institutions, airlines, telecommunications companies. 15 U.S.C. §45(a)(2).

29) 15 U.S.C. §45(m)(1)(A).

30) 15 U.S.C. §53.

31) Prepared Statement of the Federal Trade Commission On Consumer Privacy, Presented By Chairman Jon Leibowitz Before the Committee on Commerce, Science, and Transportation, United States Senate (July 27, 2010), at http://www.ftc.gov/os/testimony/100727consumerprivacy.pdf.

32) Identity theft occurs when a criminal obtains your personal information and uses it to acquire credit cards, open bank accounts, access your existing bank accounts. The FTC defines identity theft as the use of an individual's personally identifiable information, including name, bank account information, or social security number, to commit fraud or another crime.

33) http://www.ftc.gov/os/testimony/100727consumerprivacy.pdf The testimony noted that since 2001 the FTC has brought dozens of actions charging businesses with failing to protect consumers' personal information, including a complaint announced against Rite Aid Corporation, which has agreed to settle Federal Trade Commission charges that it failed to protect the sensitive financial and medical information of its customers and employees. As stated in the testimony, the FTC brought 15 actions charging website operators with collecting information from children without parents' consent, as well as 15 spyware cases and dozens of actions challenging illegal spam. http://www.ftc.gov/opa/2010/07/privacytest.shtm.

34) 15 U.S.C. §45.

35) See, e.g., News release, FTC. ChoicePoint Settles Data Security Breach Charges (Jan. 26, 2006), at http://www.ftc.gov/opa/2006/01/choicepoint.htm.

data-handling procedures constitute unfair acts or practices in violation of Section 5 of the Federal Trade Commission Act.

In the past twelve years, most of the actions the FTC has brought against individual companies have settled. The complaints have ranged from breaking promises in their privacy policies to deceptive data collection and retroactive privacy policy changes.[36] Despite some successful settlements, there is danger in relying on the FTC to comprehensively safeguard privacy interests of Internet users. The FTC's approach to regulation is necessarily ad hoc - it looks at one specific company and one particular problem at a time and can only hammer out a settlement with that company. There is no universal standard being imposed on all corporations. Also, FTC enforcement occurs one case at a time. This time frame is out of sync with the swiftness of technological developments. We see this in how quickly surveillance tools are being enhanced and replaced by more sophisticated ones. The FTC's efficacy is also hampered by the fact that it is largely a reactive agency. Rather than proactively searching for every violation of the FTC Act, the Commission sometimes is only alerted to a privacy harm when an individual or group files a complaint. This approach is overly dependent on users. Finally, the Commission appears reluctant to intervene in one of the most important aspects of the collection and use of data - companies' online tracking. Last year, the FTC released behavioral-advertising guidelines but stated in a report that, for the present time, it would maintain its self-regulation policy when it comes to behavioral advertising.[37]

Amidst the patchwork of federal legislation and ad hoc FTC enforcement actions, the states have leapt to the forefront of advocating for privacy rights. The National

---

36) See, for example, *In re Liberty Financial Cos.*, No. 9823522, 1999 FTC LEXIS 99 (May 6, 1999), *FTC v. ReverseAuction.com, Inc.*, No. 00-CV-32 (D.D.C. Jan. 6, 2000); *In re Gateway Learning Corp.*, No. C-4120 (Sept. 10, 2004).

37) Tresa Baldas, *Web Behavioral Advertising Goes to Court*, The National Law Journal, March 2, 2009, available at http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202428691751. See Liisa M. Thomas and Monique N. Bhargava, *Where Have You Been? The Rules for Online Behavioral* Advertising, Pratt Privacy & Data Security Law Journal, September 2009. ("The tracking of user's online behavior across unaffiliated websites in order to target specific ads to the user is referred to by the Federal Trade Commission as online behavioral advertising.")

Association of Attorneys General has an Internet Law task force that coordinates the enforcement of privacy. In some cases, even if the FTC did not follow up on a complaint against a specific company's privacy practices, a coalition of states compelled agreements regarding privacy policies and imposed fines on companies.[38]

In addition, every state has a statute related to either consumer protection or deceptive trade practices.[39] The language of the state statutes can be broader and more protective of users' rights than federal legislation. In fact, it has been pointed out that "even if the FTC concludes that practices pass muster under the FTC Act, it is still at least theoretically possible for a state to find the practices deceptive under their own legislation."[40] Finally, an Internet user who believes that he has been the victim of privacy violation can try to sue under a state tort, such as invasion of privacy,[41] negligence, or defamation.[42] In summary, federal regulation has been supplemented by and sometimes surpassed by state forms of redress. Despite the relative rigor of some state statutes, the fact remains, however, that not all Americans are afforded the same broad protections. There is a need therefore for a consistent federal standard that would supersede state laws, creating a comprehensive, uniform law.

---

38) For example, the FTC opened and then dropped its investigation of DoubleClick's practices of collecting and using data from and about Internet users. Plaintiffs in class action lawsuits accused the company of mixing identifying information with nonidentifiable information and profiling users without disclosing they were doing so in their posted policies. Although the FTC closed its investigation, ten states worked together to compel DoubleClick to accept a binding agreement regarding their privacy policies and disclosure and imposed a fine of $450,000 to reimburse the states for their costs. Available at http://www.clickz.com/clickz/news/1700857/doubleclick-settles-states-on-profiling

39) See, e.g., Minnesota's Deceptive Trade Practices Act, Min.. Stat. §325D.44

40) Jeff Sovern, *Protecting Privacy with Deceptive Trade Practices Legislation*, 69 Fordham L. Rev. 1305, 1352-53 (2001).

41) There are four branches of the privacy invasion tort identified by the Restatement (Second) of Torts. These are : (1) an unreasonable intrusion upon the seclusion of another; (2) an appropriation of another's name or likeness; (3) a public disclosure of private facts; and (4) publicity which reasonably places another in a false light before the public. (Restatement (Second) of Torts §§ 652B, 652C, 652D, 652E, at 378-94 (1977).

42) The majority of states also have data breach notification laws. National Conference of State Legislatures, State Security Breach Notification Laws, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm (last visited Nov. 14, 2010) (listing the notification laws).

Companies have argued that neither new state nor new federal action is necessary due to the private sector's self-regulatory regime. Currently, many companies post user agreements, which provide a box for a user to check to indicate she will abide by the terms. Alternatively, companies post privacy policy notices on their website as well as offer some form of opt-out to users. Specifically, instead of giving you the option to "opt-in" and give your permission for data collection to occur, companies generally can make users "opt-out," essentially using your information how they see fit unless you make the extra effort to turn that feature off. Many businesses often choose to follow this approach as well as voluntarily adopt codes and join privacy seal programs.[43] They argue that these voluntary standards protect users' privacy, while at the same time offering companies more flexibility than a new law. However, there is doubt as to whether consumers can have full confidence in the efficacy of such self-regulatory mechanisms. For example, TRUSTe is an e-commerce industry privacy protection organization that establishes rules for privacy policies and allows companies that follow the rules to display TRUSTe's privacy seal. When a website displays the TRUSTe stamp of approval, it is meant to signify that there has been proper disclosure of privacy policies and security practices and that a reliable third party is ensuring the website's compliance with the posted polices. This TRUSTe seal of approval was given to both Toys mart and Facebook. Both Toysmart[44] and Facebook,[45] however, in different circumstances were discovered to have violated their posted privacy policies. Users therefore should be highly skeptical of the significance of a privacy seal and the effectiveness of self-regulation mechanisms.

---

43) A "voluntary code" is a commitment made by one or more firms to abide by a stated set of practice principles. A "privacy seal program" is supposed to ensure that there is proper disclosure of a Web site's privacy and security practices and that a trusted third party is monitoring the sites' compliance with their stated policies.

44) In 2000, the Commission challenged Toysmart's effort to sell its customers' personal information, despite the promise in its privacy policy that such information would not be disclosed to a third party. See *FTC v. Toysmart.com LLC*, 00-CV-11341-RGS (D. Mass. filed July 10, 2000).

45) See http://www.facebook.com/policy.php. Research revealed that some of Facebook's most popular applications were sending users' information to outside parties, in direct violation of Facebook policies. Available at http://news.smh.com.au/breaking-news-technology/facebook-finds-apps-giving-user-id-data-to-advertisers-20101019-16r2c.html

Reviewing the laws regulating the collection and use of data by the private sector highlights the cracks in this area of the law. Federal legislation, in particular, has been largely sector oriented and unsatisfactory in fully protecting people's right to know and control the amount of data being collected on a daily basis.[46] Whether new legislation is necessary, however, depends on the importance of the privacy interests being threatened.

II. Privacy Interests at Stake

Given the fact that there has been much debate and difference of opinion about the definition of privacy,[47] it is necessary to explain how this article defines the privacy interests at stake when companies collect personal information.

The notion of privacy as having control over the dissemination to others of any personal information has deep roots. Just before the turn of the twentieth century, Samuel Warren and Louis Brandeis observed "the common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments and emotions shall be communicated to others."[48] The Supreme Court, almost a century later, agreed, stating "both the common law and the literal understandings of

---

46) Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 Fed. Comm L.J. 195, 208 (1992). ("The American legal system does not contain a comprehensive set of privacy rights or principles that collectively address the acquisition, storage, transmission, use and disclosure of personal information within the business community. The federal Constitution does not address privacy for information transactions wholly within the private sector and state constitutional provisions similarly do not afford rights for private transactions. Indeed, legal protection is accorded exclusively through privacy rights created on an ad hoc basis by federal or state legislation or state common law rules.")

47) The meaning of privacy as a value and right has been the subject of much debate and discussion. One commentator noted "even the most strenuous advocate of a right to privacy must confess that there are serious problems of defining the essence and scope of this right." William M. Beaney, *The Right to Privacy and American Law*, 31 L. & Contemp. Probs. 253, 255 (1966).

48) Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 198 (1890).

privacy encompass the individual's control of information concerning his or her person."[49]

The current system of tracking personal data by the private sector clearly dilutes this long-recognized right. Bearing in mind Daniel J. Solove's point that privacy is best understood by looking at problems contextually, the article finds three specific harms created by companies' current online practices.

1. First Privacy Harm

Solove aptly observes that "[w]hen we state that we are protecting 'privacy,' we are claiming to guard against disruption to certain practices."[50] Here, people's settled expectations are being disrupted in an unprecedented way. The first privacy harm is grounded in the fact that people have long thought of the books they read, the items they buy, the relationships they have, their thoughts, fears, and hopes, as private. Traditionally people in America have believed themselves to be able to, with minimal intrusions on their privacy, learn information, create friendships, and purchase products, all without worrying about these details being collected and bartered. These activities typically were done in libraries, stores, offices, and homes with relative anonymity. Although of course there was rarely absolute privacy in the sense that usually at least one person, e.g., the librarian at the library, knew of your interest in mythology or cartoons,[51] your reading preferences were not being systematically compiled into an online profile nor used for targeted advertising. Now companies have troves of details about us and may disseminate such information to a third party like a data broker. Allowing third parties access to personal information disturbs an individual's sense of autonomy.

The fact that these third parties are not known or chosen by individuals to be

---

49) *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989).

50) Solove, supra at 1129.

51) Id. at 1109. ("We often expect privacy even when in public. Not all activities we deem as private occur behind the curtain. The books we read, the products we buy, the people we associate with − these are often not viewed as secrets, but we nonetheless view them as private matters.")

privy to this information compounds the problem. Most individuals once had the freedom to decide how much and what type of information to entrust to specific people. Some of the information we reveal in searches, for example, are things we may have shared with friends and family and maybe a professional such as a doctor or attorney; however, we exerted control over this disclosure process. In this way, people traditionally felt as if they could determine the level of intimacy in a relationship − in part by sharing or withholding their thoughts, feelings, and interests. Although these categories of information may not have been considered secrets, it was felt by an individual to be private. Eric Schmidt, Chief Executive of Google, once defended how the company views private information by saying "[i]f you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."[52] Schmidt misunderstands the privacy problem. There is much information an individual considers private, but that he or she knows is neither shameful nor illicit. Current online practices, however, strip away an individual's freedom to choose who will know his private thoughts and sentiments. Now people who have never met you have access to details about the stresses of your job, concerns about your parent's health, and more. Knowing that your every online query and behavior are being tracked by unknown people diminishes an individual's sense of freedom to have his own space without feeling the pressure of being monitored or even judged.[53]

---

52) Nick Bilton, *Consumer Group Aims at Google*, The New York Times, September 6, 2010.

53) Julie E. Cohen, *Examined Lives: Informational Privacy and The subject as Object*, 52 Stan.L.Rev. 1373, 1425-1426 (2000). ("The universe of all information about all record-generating behaviors generates a 'picture' that, in some respects, is more detailed and intimate than that produced by visual observation, and that picture is accessible, in theory and often in reality, to just about anyone who wants to see it. In such a world, we all may be more cautious. The point is not that people will not learn under conditions of no-privacy, but that they will learn differently, and that the experience of being watched will constrain, ex ante, the acceptable spectrum of belief and behavior. Pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream. The result will be a subtle yet fundamental shift in the content of our character, a blunting and blurring of rough edges and sharp lines.") See also Jonathan Shaw, *Exposed, The erosion of privacy in the Internet era*, Harvard Magazine, September-October 2009, at http://harvardmagazine.com/2009/09/privacy-erosion-in-internet-era ("There is always the possibility that we will decide as a society not to support privacy. Harry Lewis believes that would be society's loss. 'I think ultimately what you lose is the development

2. Second Privacy Harm

The second privacy harm posed by tracking online behavior is the disempowerment of individuals. Rather than being able to define themselves, users feel as if someone else is defining them. What is worse is that this someone else is not a person who has a past history with you and knows you but is nameless and faceless. They are not your local librarian or your personal physician. Knowing that there are detailed dossiers being created impairs individuals' sense of dignity and personhood. When these profiles are used to send targeted advertisements, an individual may feel pigeonholed or stereotyped.[54] By way of contrast, when the same individual used to borrow a golf book from the library, even if the librarian thought she knew what his interests were, the librarian did not, every time he subsequently entered the library, hold up a prominent blinking sign for golf books and golf magazines.

An additional risk is that, based on their databases and online profiles, companies may make decisions about us that we would never anticipate or want. For example, most people understand that whether or not they pay their bills on time affects their credit reports. But they would be surprised to learn that what establishments they frequent is also considered.[55] Similarly, companies are already trying to sell to

---

of individual identity,' he says. 'The more we are constantly exposed from a very young age to peer and other social pressure for our slightly aberrant behaviors, the more we tend to force ourselves, or have our parents force us, into social conformity. So the loss of privacy is kind of a regressive force. Lots of social progress has been made because a few people tried things under circumstances where they could control who knew about them, and then those communities expanded, and those new things became generally accepted, often not without a fight. With the loss of privacy, there is some threat to that spirit of human progress through social experimentation.'")

54) See, e.g., Joseph Turow, Annenberg Pub. Policy Ctr. of the Univ. of Pa., Americans and Online Privacy: The System Is Broken (2003), 8, available at http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf ("Inferences drawn from demographics and web-surfing habits can encourage discrimination in the kinds of editorial and advertising materials a site shows consumers. Such activities will become more intense as technologies to mine data, analyze data, and tailor based on the conclusions become more efficient and costeffective. As they expand, the activities may well lead people to feel anxious not only that they are being tracked but that they are being treated differently − for example, given different discounts − than others because of who they are and what their "clickstream" says about them.")

55) Charles Dunigg, *What Does Your Credit-Card Company Know about You?*, The New York

banks information about an individual's social network to influence credit decisions.[56] The theory is that creditworthy people would generally be friends with credit worthy people.[57] This practice raises the specter of an individual being stereotyped by companies relying on assumptions and generalities. There are no concrete legal limits on how to use personal information.

The presumption that, based on their algorithms, companies can tell who an individual is and what he would be likely to do does more than undermine a person's sense of autonomy. It ignores the dynamic nature of individuals. People are constantly evolving and changing they can become more adventurous or more settled, more conservative or more liberal, develop new habits or retire old habits. Blatantly disregarding this possibility in creating online profiles and targeting ads based on prior searches further deprives the individual of the ability to define himself.

Another problem related to the proliferation of online dossiers is that companies may mistakenly mischaracterize a person. This risk was demonstrated in news report about the startling identification of a woman based on her internet activity over AOL. In the summer of 2006, a journalist's investigation determined that one individual (identified only as user No. 4417749 in a list of 20 million Web search queries collected by AOL and released on the Internet) was really Thelma Arnold. Heridentity was inferred by studying AOL records of her searches within the span of three months.[58] There were queries for "landscapers in Lilburn, Ga," several people with

---

Times, May 12, 2009. Dunigg reported that a Canadian credit-card issuer had discovered that people who used their card in a particular pool hall in Montreal had a 47 percent chance of missing four bill payments during the subsequent 12 months, whereas people who bought anti-scuff felt pads for the legs of their furniture almost never missed payments.

56) Angwin, supra.

57) Companies frequently use advanced algorithms to mine user data and create an online profile. The algorithms work by creating inferences about an individual's personality, which are partially based on stereotypes. See Nancy J. King, *When Mobile Phones Are RFID-Equipped − Finding E.U.-U.S. Solutions to Protect Consumer Privacy and Facilitate Mobile Commerce*, 15 Mich. Telecomm. Tech. L. Rev. 107, 145 (2008) (citing Mireille Hildebrandt, *Profiling into the Future: An Assessment of Profiling Technologies in the Context of Ambient Intelligence*, 1 FIDIS J. of Identity in the Info. Soc'y 7 (2007)).

58) Michael Barbaro and Tom Zeller Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, The New York Times, August 9, 2006.

the last name Arnold, “mature living” and “homes sold in shadow lake subdivision Gwinnett County Georgia.” It did not take much investigating for the journalist to deduce that the user was Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga. The case made clear how personal information, if cumulatively analyzed and cross-referenced, could reveal an individual’s identity. However, the discovery also made clear that in Thelma Arnold’s case, user’s searches could prove highly misleading. For example, although Arnold had conducted searches on nicotine, dry mouth, and bipolar, seeming to indicate various health problems, it turns out that these searches had been made out of concern for various friends. Such misinterpretations of data undoubtedly occur with other users as well. Due to the very real prospect that their search data could be misleading, users at a minimum need to be able to check the accuracy and completeness of their online profiles and correct, update, or delete details in them.

Companies have argued that even when personal data is collected, since this data is anonymized, there is no danger to the privacy of an individual.[59] However, this argument loses ground as research begins to show that so-called personally identifiable information (PII) and other information collected about an individual is increasingly hard to distinguish.[60] This is because, as Thelma Arnold shows, the accumulation of data on individuals at this point is so dense that one, with reasonable amount of time and energy, has a high likelihood of figuring out from anonymized data who a

---

59) Traditionally private companies have emphasized their ability to “anonymize” data such that data which may have been personally identifiable no longer could be.

60) Shaw, supra. (“If you tell Latanya Sweeney ··· nothing about yourself except your birth date and five-digit zip code, she’ll tell you your name. If you are under the age of 30 and tell her where you were born, she can correctly predict eight or nine digits of your nine-digit Social Security number. ‘The main reason privacy is a growing problem is that disk storage is so cheap,” says the visiting professor of computer science, technology, and policy at CRCS. “People can collect data and never throw anything away. Policies on data sharing are not very good, and the result is that data tend to flow around and get linked to other data.’ ··· Fully 87 percent of the United States population is uniquely identified by date of birth, five-digit zip code, and gender, she says: ‘So if I know only those three things about you, I can identify you by name 87 percent of the time. Pretty cool.’ In fact, Sweeney’s ability to identify anyone is close to 100 percent for most U.S. zip codes···”)

particular individual is. In fact, one research scientist points out that typically all that's needed to uniquely identify one person is a total of 33 "bits" of information about him or her.[61]

Moreover, there is enough ambiguity and disagreement about what is and should be publicly available information and what should not be that some websites are changing their policies regarding this distinction, leading to users' confusion.[62] At the same time that websites can redefine what is considered to be publicly available information, newly developed software tools have the ability to re-identify supposedly anonymized data. In July 2010, Jon Leibowitz, Chairman of the Federal Trade Commission testified in front of Congress that because of the advent of such software, "the distinction between personally identifiable information ('PII') and non-PII is losing its significance. Thus, information practices and restrictions that rely on this distinction may be losing their relevance."[63]

3. Third Privacy Harm

The diminishing ability of users to feel as if they can remain anonymous online is related to the third privacy harm posed by online profiling. The level of detail in online dossiers which, as of this writing, is increasing still, is vulnerable to rising data security risks.[64] Researchers have shown how just providing your date of birth

---

61) Emily Steel and Julia Angwin, *On the Web's Cutting Edge, Anonymity in Name Only*, The Wall Street Journal, August 4, 2010.

62) Kevin Bankston, *Facebook's New Privacy Changes: The Good, The Bad, and The Ugly*, December 9, 2009, at http://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly (Under the new privacy policy, Facebook treats list of friends − "along with your name, profile picture, current city, gender, networks, and the pages that you are a 'fan' of − as 'publicly available information' or 'PAI.' Before, users were allowed to restrict access to much of that information. Now, however, those privacy options have been eliminated. For example, although you used to have the ability to prevent everyone but your friends from seeing your friends list, ··· that old privacy setting has now been removed completely from the privacy settings page.")

63) Available at http://www.ftc.gov/os/testimony/100727consumerprivacy.pdf

64) Shaw, supra. ("There is a pitched battle going on in cyberspace that pits an organized criminal ecosystem of "phishers," "money-mules," and "cashiers" against a jumbled array of private "take-down" firms, official domain-name registrars, and Internet service providers. As Tyler Moore, a postdoctoral fellow at Harvard's Center for Research on Computation

and hometown can provide a potential identity thief with your Social Security Number.[65] Moreover, the wealth of detail in the hand of private companies is an increasingly tempting target to cyber criminals.

This problem of having such massive amounts of data is compounded by the fact that cyber attacks have become more sophisticated.[66] Just as importantly, the rate of cybercrime has increased.[67] Although the FTC has investigated specific data

---

and Society explains…, the bad guys take over personal computers not for their information, but for their processing power, using "botnets" to stage "fast-flux" attacks that conceal their identity even as they steal the keys to their victims' bank accounts.")

65) Id. ("A potentially even more serious privacy crisis looms in the way Social Security numbers (SSNs) are assigned, Sweeney says. 'We are entering a situation where a huge number of people could tell me just their date of birth and hometown, and I can predict their SSN. Why is this a problem? Because in order to apply for a credit card, the key things I need are your name, your date of birth, your address, and your SSN. Who is the population at risk? Young people on Facebook … Facebook asks for your date of birth and hometown, two pieces of information that most young people include on their pages simply because they want their friends to wish them a happy birthday. The problem is that SSNs have never been issued randomly − the first three digits are a state code, the second two are assigned by region within state − and the process is described on a public website of the Social Security Administration. Starting in 1980, when the Internal Revenue Service began requiring that children have SSNs to be claimed as dependents on their parents' tax returns, the numbers started being assigned at birth. Thus, if you know a person's date and location of birth, it becomes increasingly simple to predict the SSN.")

66) Id. ("Allan Friedmannotes that computers running the first version of WindowsXP will be discovered and hacked, on average, in less than four minutes, enabling the criminal to take control of the system without the owner's consent or knowledge … botnets − networks of machines that have been taken over − find vulnerable systems through brute force, by testing every address on the Internet, a sobering measure of the scale of such attacks.")

67) In 2009 alone, the Internet Crime Complaint Center (IC3) received 336,655 complaint submissions, which was ultimately a 22.3% increase from the previous year and a 571% increase over the previous nine years when the IC3 was first created. Just as bad, the monetary damages are increasing as well: nearly 560 million dollars worth, which is over well over a 200% increase from the previous year. Available at http://www.techi.com/2010/06/the-dark-side-of-technology/. See also Symantec 2010 State of Enterprise Security Study Shows Frequent, Effective Attacks on Worldwide Business (Symantec Corp. released the findings of its global 2010 State of Enterprise Security study. It found that : every enterprise (100 percent) experienced cyber losses in 2009. The most prevalent three reported losses were theft of intellectual property, theft of customer credit card information or other financial information, and theft of customer personally identifiable information.

breaches of some companies, its power is limited. Moreover, it acts on an ad hoc basis against a specific company each time. There is no assurance to users that their data is being safeguarded from identity thieves and other cybercriminals in a consistent and rigorous manner. Individuals who provide their personal information to companies, however, should be entitled to expect that their information will be protected.

III. Ticking Time Bomb

Although there has been intermittent efforts to draft legislation to protect users' privacy, countervailing forces, including industry lobbying as well as a traditional reliance and focus on self-regulation, have thus far prevailed.[68] One commentator has stated that "it is now clear that industry lobbying has succeeded while self-regulation has failed…"[69] Other commentators have noted that the traditional justification for privacy (that its importance lies in the value it has to an individual) has provided poor basis for public policy and that there should be a push to recognize the social or community value of privacy to create a more effective public policy to protect privacy.[70] In 1995, Congress did provide a modest response to growing requests for consumer privacy protection and asked the Federal Trade Commission to become involved with consumer privacy issues.[71] The FTC, however, in some ways has

---

These losses translated to monetary costs 92 percent of the time. The top three costs were productivity, revenue, and loss of customer trust. Enterprises reported spending an average of $2 million annually to combat cyber attacks.) Available at http://www.symantec.com/about/news/release/article.jsp?prid=20100221_01.

68) Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 Fed. Comm. L.J. 195 (1992) ("traditional American fear of government intervention in private activities and the reluctance to broadly regulate industry").

69) Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 Md. L. Rev. 140, 172-173 (2007). See also Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry doesn't Get)*, 2001 Stan. Tech. L. Rev. 1, 117-19.

70) Priscilla M. Regan, Legislating Privacy : Technology, Social Values, and Public Policy (1995).

71) Daniel J. Solove & Paul M. Schwartz, *Information Privacy Law*, Aspen Publishers (3rd

merely prolonged the view that self-regulation, in large part, is sufficient. The FTC posited that privacy policies and notices, key aspects of any self-regulation framework, should be sufficient protection without unduly burdening the innovation and profitability of businesses. Supporters of this approach have pointed to industry studies as supporting the fear that privacy protection measures, such as comprehensive legislation, impose heavy costs on companies.[72)]

Another argument that companies collecting personal data make is that users do not seem, as a whole, to even want privacy very much.[73)] Various commentators have noted that many Americans seem willing to give up privacy for coupons or services or ease of use and generally fail to adopt software and other technology that would protect their privacy.[74)]

In recent years, however, an increasing number of people express concern about privacy on the Internet. A national poll found that most American consumers want online privacy and that over 80% of Americans are concerned about the security and privacy of their personal information on the Internet; about 90% of Americans consider some common industry behaviors to be unfair business practices; and about 80% of Americans support a variety of stronger consumer protections of their privacy online.[75)] Similarly, a 2008 nationwide survey by Harris Interactive and Alan F. Westin found that consumers are uncomfortable with information about their online activities being used to better target advertisements. 59% of respondents were

---

ed, 2009), 776.

72) See, e.g., Michael E. Staten & Fred H. Cate, *The Impact of Opt-In Privacy Rules on Retail Credit Markets : A Case Study of MBNA*, 52 Duke L.J. 745, 767-68 (2003).

73) Anita L. Allen, *Coercing Privacy*, 40 Wm. & Mary L.Rev. 723, 737 (1999). (“for people under forty-five who understand that they do not, and cannot, expect to have many secrets, informational privacy may now seem less important. As a culture, we seem to be learning how to be happy and productive − even spiritual − knowing that we are like open books, our houses are made of glass…”)

74) See, e.g., Eric Goldman, *The Privacy Hoax*, Forbes (Oct. 14, 2002).

75) Scott Cleland, *Americans want online privacy − per new Zogby poll*, June 8, 2010, available at http://precursorblog.com/content/americans-want-online-privacy-new-zogby-poll. See also Joseph Turow, Americans & Online Privacy The System is Broken A Report from the Annenberg Public Policy Center of the University of Pennsylvania June 2003, 17, available at http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf.

not comfortable with websites like Google, Yahoo, and MSN using information about their online behavior to tailor content to their interests, even though the question indicated that the practice allowed them to offer e-mail and other services for free.[76] Another survey found that this discomfort existed even if the information collected was made anonymous.[77]

Even younger users, such as teenagers, appear to be showing a reenergized interest in privacy. A majority in a survey reported that they have taken steps to protect their profiles on social networking sites such as Facebook. According to a Pew Research Center study, sixty-six percent of teenage social network users reported that their profile is not visible to all internet users.[78] The recent privacy controversies trailing Facebook may have prompted some users to be more proactive about their privacy settings. It also may have contributed to reported low customer satisfaction with Facebook.[79]

---

76) Available at http://www.cdt.org/privacy/guide/surveyinfo.php. See also Joseph Turow, Jennifer King, Chris jay Hoofnagle, Amy Bleakley, Michael Henessy, Contrary to what marketers say, Americans reject tailored advertising, and three activities that enable it, September 2009.

77) *Most Americans dislike behavioral advertising : survey*, September 30, 2009, available at http://www.physorg.com/news173555711.html (Eighty-six percent of the young adults said they do not want tailored advertising if it is the result of following their behavior on websites other than the one they are visiting. Sixty-eight percent of those surveyed said they "definitely" would not allow themselves to be followed on websites even if it was being done anonymously while 19 percent said they would "probably" not allow it.") Also, a poll released by Zogby International earlier this summer found that 80 percent of U.S. adults are concerned with companies recording their online habits and using the data to generate profit through advertising, while 79 percent already support a national "Do Not Track List." Available at http://www.socialtimes.com/2010/10/government-policy-on-internet-privacy/

78) Pew Internet and American Life Project, Teens, Privacy, and Online Social Networks, available at http://www.pewinternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.spx?r=1.

79) In a recent study by Foresee Results and the University of Michigan, Facebook scored extremely low in the area of customer satisfaction. The 2010 American Customer Satisfaction Index E-Business Report included social networking companies for the first time, and Facebook scored a 64, putting it "in the bottom 5% of all measured private sector companies and in the same range as airlines and cable companies." The polling company attributed Facebook's low scores to "privacy concerns, frequent changes to the website, and commercialization and advertising." http://www.businesswire.com/news/home/20100720005040/en/Facebook-Flops-ACSI-E-Business-Report

To the extent that some users do not express much concern about privacy, this article posits that this attitude at least partly stems from a lack of awareness of the extent of the information gathering, and the accompanying implications. The question to explore therefore is what do users generally know about their privacy online.

Surveys and analysis make clear that many people are still not fully informed as to how the data is being collected or used.[80] In FTC sponsored roundtable discussions,[81] participants, who included industry insiders and consumer groups and academics, expressed concern that data collected for one purpose can be combined with other data and then used for purposes not anticipated by the consumer. Participants also worried that users were unaware that companies such as data brokers routinely collect and sell such aggregated data.[82]

Moreover, many users do not know the extent to which they are being monitored and the sophisticated tools being deployed to do that. A Consumer Policy Solutions survey[83] found that consumers think they are knowledgeable about online privacy, but many are unaware of how their activity and behaviors can be shadowed online.[84]

A few months ago, a Wall Street Journal study revealed that the tracking of consumers has grown much more invasive than most people realize. The Journal identified more than 100 middlemen in between the Internet user and the advertiser - tracking companies, data brokers and advertising networks − all competing to buy

---

80) See, e.g., Joseph Turow, Americans & Online Privacy The System is Broken A Report from the Annenberg Public Policy Center of the University of Pennsylvania June 2003, 19, 21 available at http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf. A majority in one national survey stated their belief that the mere fact that a company had a posted privacy policy meant that a website would not share personal information with other companies.

81) http://www.ftc.gov/os/testimony/100727consumerprivacy.pdf announced late last year that it would examine consumer privacy in a series of public roundtables. Over 200 representatives of industry, consumer groups, academia, and government agencies participated in the roundtables, and the Commission received over 100 written comments.

82) Available at http://www.ftc.gov/os/testimony/100727consumerprivacy.pdf

83) Survey was conducted by Peter D. Hart Research Associates, Consumer Awareness Project.

84) Available at http://www.cdt.org/privacy/guide/surveyinfo.php; the survey specifically found: 42% are unsure whether their online activity is tracked and recorded by companies for commercial purposes. Only 30% have read online retailers' privacy policies closely and only 18% have read search engine privacy policies closely.

and sell data on individual behavior and interests.[85] Many users do not know how much personal data is being gathered about them via spying on their searching and browsing habits to create profiles, some of which are "eerily correct."[86] They are unaware that what they type into search browsers is compiled into profile to be sold to the highest bidder.

Without an understanding of the surveillance tools, as well as the potential uses of their data, people cannot give fully informed consent regarding giving up their data. Most people are also unaware that risks to their privacy will be magnified when a new website programming code, HTML5, powers the internet.[87]

In addition to needing more explanation about tracking tools, users need to understand that the level of detail now being collected by companies enables, at least in some cases, for the possibility of being identified. Some users may not express much worry about online privacy because they do not think anything that could personally identify them is being bartered or sold. Nevertheless, as Solove points out, "[a]n individual may giveout bits of information in different contexts, each transfer appearing innocuous. However, the information can be aggregated and could prove to be invasive of the private life when combined with other information. It is the totality of information about a person and how it is used that poses the greatest threat to privacy."[88] The AOL case made clear that if enough details about one's life, interests, thoughts, and habits are gathered, the details as a whole can be used to identify the individual.

Thus, even if users consent to the user agreements related to privacy on some

---

85) Angwin, supra.

86) Id.

87) Tanzina Vega, *Web Code Offers New Ways To See What Users Do Online*, The New York Times, October 11, 2010. ("The new Web language and its additional features present more tracking opportunities because the technology uses a process in which large amounts of data can be collected and stored on the user's hard drive while online. Because of that process, advertisers and others could, experts say, see weeks or even months of personal data. That could include a user's location, time zone, photographs, text from blogs, shopping cart contents, e-mails and a history of the Web pages visited.")

88) Daniel J. Solove, *Privacy and Power : Computer Databases and Metaphors for Information Privacy*, 53 Stan.L.Rev. 1393, 1452 (2001).

websites, their consent is not always informed. There is aninformation asymmetry between users and the companies that collect their data about the types of tracking tools, the uses of the data, and the extent of the data collected that creates a power imbalance. This power imbalance has yet to be addressed effectively.

Finally, those users who try to take active steps to protect their online privacy may be thwarted in their good faith attempts. Some users carefully read the entire privacy policy posted on a website but have difficulty understanding the nuances of the company's practices. The length and complexity of the privacy polices is almost reminiscent of the fine print in credit card contracts, which Elizabeth Warren described as incomprehensible. In the context of credit applications, Warren commented, "I am a contract law professor, and I cannot understand some of the fine print [in credit card contracts]."[89] By the same token, the convoluted lengthy passages about privacy posted on company websites can be almost indecipherable.

A user trying to protect his privacy may encounter more obstacles when he uses tools and changes settings to effectively block tracking. Several class-action lawsuits have been filed this year alleging that companies gathered information on the websites that users visited and from the videos they watched, although the users had selected privacy settings in the web browser to reject cookies that could track them. The problem, plaintiffs say, is that while they were able to get rid of HTML cookies,[90] they could not erase flash cookies, which are stored in a separate directory that many users are unaware of and may not know how to control.[91] One of the

---

89) See Regulatory Restructuring : Enhancing Consumer Financial Products Regulation: Statement Before the H. Comm. on Financial Servs., 111th Cong. (2009) (statement of Elizabeth Warren). Warren points out that "…terms hidden in the fine print or obscured with incomprehensible language, unexpected terms … and similar tricks and traps have no place in a well-functioning market." Elizabeth Warren, *Unsafe at Any Rate*, Democracy Journal, Issue #5, Summer 2007.

90) HTML cookies store Web site preferences and can be managed by changing privacy settings in a Web browser.

91) Tanzina Vega, *Code That Tracks Users' Browsing Prompts Lawsuits*, The New York Times, September 21, 2010. See also Riva Richmond, *Resisting the Online Tracking Programs*, New York Times, November 11, 2010 ("…advertisers are increasingly using powerful software known as supercookies, such as so-called Flash and document object management (or DOM) cookies, which can hold more information, and Web bugs or beacons, which let sites

plaintiffs, Ms. Person Burns, 67, a retired health care executive, tried to block all tracking devices on her computer, only to learn that flash cookies had not been blocked. Burns said she is now wary of online shopping: "Instead of going to Amazon, I'm going to the local bookstore." Another problem for those trying to prevent behavioral tracking is found in the loopholes in some coding. For example, researchers at CyLab at the Carnegie Mellon University School of Engineering discovered that even if you set Internet Explorer to block cookies, large numbers of websites, including Facebook, appeared to be using a loophole that circumvents Explorer's ability to block cookies.[92)]

Sometimes it is not only users who are surprised by some of the tracking practices of companies. Significantly, companies themselves sometimes are not aware of what data they are collecting, both data long considered sensitive and other data. In May of 2010, Google acknowledged that for years it had, through its "Street View" cars photographing neighborhoods for Google's street views, inadvertently picked up personal data − which a security expert said at the time could have included e-mail messages and passwords − sent by consumers over wireless networks.[93)] Moreover, Facebook last month dealt with another privacy controversy when The Wall Street Journal reported that ten popular applications on Facebook transmitted personal information about users and user's friends to outside companies (such as advertising and Internet tracking companies) in violation of Facebook's privacy policy[94)] − and

---

record statistics like what ads attracted you to the site and whether you bought something. They are not removed when you clear out your cookies.")

92) Riva Richmond, *False Sense of Security*, The New York Times, September 20, 2010. ("About one third of the more than 33,000 sites they studied have technical errors that cause I.E. to allow cookies to install, even if the browser has been set to reject them. Of the 100 most visited destinations on the Internet, 21 sites had the errors, including Facebook, several of Microsoft's own sites, Amazon, IMDB, AOL, Mapquest, GoDaddy and Hulu.")

93) *States to Investigate Google Data Collection*, Reuters, June 21, 2010. ("'It was a mistake for us to include code in our software that collected payload data, but we believe we did nothing illegal. We're working with the relevant authorities to answer their questions and concerns,' a Google spokeswoman, Christine Chen, said in an e-mail message.")

94) Facebook specifically prohibits applications makers from transferring data about users to outside advertising and data companies, even if a user agrees. Available at http://news.smh.com.au/breaking-news-technology/facebook-finds-apps-giving-user-id-data-to-advertisers-20101019-16r2c.html

sometimes even their own policies.[95] The recipients included data firms that build profiles of Internet users by tracking their online activities. The Wall Street Journal reported that the problem affected tens of millions of Facebook application users, including those who set their profiles to be completely private.[96]

Some of the biggest American websites have also appeared to be caught off guard when a Wall Street Journal article revealed the number and type of intrusive files being installed on visitors' computers.[97] For example, the Journal discovered that Microsoft Corporation's web portal, MSN.com, planted a tracking file full of data - it predicted a surfer's age, zip code, gender, estimates of income, marital status, presence of children, and home ownership. Both the tracking company that created the file and Microsoft said they did not know how the file got onto MSN.com. The fact that some of the most popular websites in America do not know and could not control the amount of data being gathered by third parties such as advertising networks, makes clear that self-regulation does not work.

Unintentionally failing to adhere to posted privacy policies risks not only violating users' privacy expectations but also endangers the security of the data. Researchers, for example, have found that companies do not always delete hard drives of sensitive data before discarding them.[98]

Given the numerous vulnerabilities associated with personal data in the hands of companies and data brokers, consistent across-the-board regulation of the collection of personal information is necessary. The fact that even some of the most sophisticated companies are failing to follow their policies, however inadvertently, suggests that it's only a matter of time before the data could be inappropriately accessed or

---

95) AJ Glasser, *Zynga gave advertisers user info*, The Wall Street Journal, October 18, 2010.

96) *Facebook finds apps giving user ID data to advertisers*, October 19, 2010. Available at http://news.smh.com.au/breaking-news-technology/facebook-finds-apps-giving-user-id-data-to-advertisers-20101019-16r2c.html

97) Angwin, supra.

98) Shaw, supra. ("Simson Garfinkel, now an associate of the School of Engineering and Applied Sciences and associate professor at the Naval Postgraduate School, reported in 2003 that one-third of 1,000 used hard drives he had purchased on eBay and elsewhere still contained sensitive financial information. One that had been part of an ATM machine contained thousands of credit-card numbers. It had not been properly 'wiped' of its data.")

misused. The federal government once thought it was best to only lightly regulate consumer financial products and mortgage lending because the situation initially appeared to be under control. Just as the deregulatory zeal in that area helped effectuate a crisis, here the lack of comprehensive regulation in the face of increasing stockpiles of personal data, creates the equivalent of a privacy time bomb.

IV. Proposal

This article recognizes that companies offer free services and content to Internet users and have a business interest in monetizing data. Moreover, any new legislation should be cognizant of the need to encourage the private sector to continue to innovate. It should also be noted that some of the technological software, such as cookies, enhances the user's experience. Cookies in their most basic form store details of the user's activity on that site. This enables the site's server to recognize the computer the next time it visits, so that the user will be provided with the same layout, shopping cart, and personalized greetings and settings. However, the argument that cookies are benign and only used to help users is disingenuous. As the Wall Street Journal's investigation demonstrated, over two-thirds of the 3,180 tracking files placed on a user's computer by the most popular 50 American websites (which represent 40% of the Web pages viewed by Americans) were installed by 131 middlemen companies trying to track users' activities on the Internet to sell as profiles.

Moreover, companies clearly are reaping the benefits of using personal data to better market, advertise, and make profits; any tracking activity should therefore impose responsibilities on the companies as well. This responsibility should include agreeing not to lend, sell, or share personal information with third parties without the user affirmatively opting-in. The companies should also be required to have strong data security programs in place, particularly as many individuals are still oblivious as to the amount of detail collected about them, and how such data could be used to identify them.

Federal legislation is therefore necessary to uniformly regulate the collection of data by the private sector. Rather than proposing radical changes, the legislation would set forth a minimum standard of legal protection. Moreover, to ensure that the legislation could be implemented with minimal disruption to company's operations, the bill would be drafted with active participation and input of technological and software experts. The federal statute would include mandating that companies provide clear, concise privacy notice displayed somewhere on the home page. This should be a summary of the key facts, and separate from the more detailed privacy policy that may be too lengthy for most users to read thoroughly. This would also mandate what the FTC in its ad hoc authority has already indicated that merely including a disclosure about tracking within the body of a company's privacy policy may not be sufficiently clear and prominent.[99] Unlike today, when some websites have such long, complicated instructions as to which aspects of your use of the site can be made private that even tech savvy users are frustrated,[100] notices going forward should be clearly written. The notice would describe how information is collected, what data is being collected, how company is using data, whether and to what extent they share, loan, or sell this data to third parties. In addition, companies would no longer be able to force users to opt-out of any sharing or selling of data to third parties. Rather, companies would have to request and obtain users' consent before doing so. Users would also have the ability to look at the personal

---

99) Liisa M. Thomas, Balancing Technology and Power : Emerging Rules in Online Behavioral Advertising, Mobile Marketing, Social Networking, and Other Electronic Commercial Communications, Presentation at PLI's Eleventh Annual Institute on Privacy and Data Security Law, Chicago (July 2010). (The FTC has noted that "privacy policies have become longand difficult to understand, and may not be an effective way to communicate information to consumers.")

100) Danny Sullivan, editor-in-chief of Search Engine Land, a blog that covers news and information about search engines and search engine marketing, wrote of the recent changes to the Facebook privacy settings : "Your product should speak clearly for itself. I shouldn't have to dive into complicated settings that give the fiction of privacy control but don't, since they're so hard to understand that they're ignored. I shouldn't need a flowchart to understand what friends of friends of friends can share with others. Things should be naturally clear and easy for me." Danny Sullivan, Dear Facebook & Google: We Are Not Your Pawns − Enough With The Auto Opt-In!, Daggle, April 23, 2010, available at http://daggle.com/dear-facebook-google-pawns-optin-1796.

information the company has compiled thus far and correct or delete any information. Moreover, the legislation would mandate the FTC's recommendation that express consent from users would be required before material retroactive changes to privacy policy are imposed.[101] Just as the Gramm-Leach-Bliley Act ("GLB")[102] provides, the legislation should authorize agencies such as the FTC to establish data security standards for nonpublic personal information.[103] These should include ensuring that companies have policies to delete search data after a certain set period. Finally, the federal statute would make clear that it would preempt state legislation related to the use of personal data by companies except to the extent that the state statute provides stronger protections for users.

The proposed legislation here is similar in some ways to the Boucher-Stearns bill, but stronger. Rick Boucher, former chairman of the House Subcommittee on Communications, Technology and the Internet, and the chief advocate of the Boucher-Stearns bill,[104] lost his seat in the recent midterm elections. The fate of the bill is therefore is uncertain.[105] However, parts of the bill should be incorporated

---

101) Available at http://www.ftc.gov/os/testimony/100727consumerprivacy.pdf

102) Financial Services Modernization Act, Pub. L. No. 106-102, codified at 15 U.S.C. §§6801-6809.

103) GLB provides this in 15 U.S.C. §§6801(b), 6805(b)(2). (financial institutions "shall develop, implement, and maintain a comprehensive information security program" that is appropriate to the "size and complexity" of the information, the "nature and scope" of the institution's activities, and the "sensitivity of any customer information at issue.") 16 C.F.R. §314.3(a).

104) The Boucher-Stearns proposed legislation would require companies to get a user's explicit approval (that is, it would require users to "opt in") before they "knowingly collect" information about a person's medical history, financial records, Social Security number, sexual orientation or precise geographic location. Other information, such as that collected by web cookies or session logs on corporate servers, would not require explicit consent, provided the company involved displays a "clearly-written, understandable privacy policy that explains how information about individuals is collected, used and disclosed" and provided users can decline or "opt out."

105) In July, Representative Bobby L. Rush, Democrat of Illinois, introduced an online privacy bill that would, among other things, require companies to disclose how they collect, use and maintain the personal information on users and to make those disclosures easy for users to understand. Tanzina Vega, *Code That Tracks Users' Browsing Prompts Lawsuits*, The New York Times, September 21, 2010.
Either Rush's bill or some form of Boucher-Stearns bill may be taken up by Congress

into new legislation whereas other parts should be left out. Under the Boucher-Stearns bill, companies have to disclose the fact that they are part of an advertising network and when information is collected by one website it can be shared across the network. Anytime information is shared beyond the immediate party that collected it, then companies have to seek the consent of the user. However, the advertising network can quality for opt-out treatment if it does other things, such as giving users the opportunity to access a collective preference profile and modify the profile.[106)]

In contrast, this article recommends that federal legislation provide for no such exemption but that consent is required by users if information is loaned/sold/shared with any third party. Moreover, new legislation should mandate that all corporations offer users a way to check their online dossier and, as necessary, amend it.

Finally, the legislation should, unlike the Boucher-Stearns bill, make a concerted effort to include in its purview mobile broadband, something that has been largely flying under the radar of the drafters of the Boucher-Stearns bill.[107)]

Under the new legislation, some companies may have to change only parts of their current practices. For example, a few websites currently will disclose to you what they know about you or think they know (Google, Microsoft, and Yahoo, have created “preference managers” that let users view and modify or correct the interests they've assigned to you based on your browsing behavior.)[108)] Yahoo and Google also have “back-end privacy protections” in that they control how much data they keep and for how long. Yahoo holds search data for 90 days for the majority of log

---

next year as both Democrats and Republicans in Congress have called for companies to address claims of privacy intrusion and breaches.

106) Interview with Rick Boucher and Cliff Stearns, on C-Span, the Communicators, (Oct. 2, 2010) [hereinafter C-Span interview), available at http://www.cspan.org/Watch/Media/2010/10/02/HP/A/38840/Reps+Rick+Boucher+DVA+and+Cliff+Stearns+RFL.aspx.

107) C-Span interview (Rep. Stearns said in CSpan interview that draft bill does not focus on mobile broadband but focuses on computers although he also acknowledged that the future would be computer/book/movie station/camera/phone device.)

108) Riva Richmond, *Resisting the Online Tracking Programs*, The New York Times, November 11, 2010 (“Google, Yahoo and online data exchanges BlueKai, Bizo and Rapleaf will show you what interests − such as cars, travel or beverages − they believe you have, and let you delete them. They also let you opt out of getting ‘interest-based’ ads altogether.”)

files (not just search but others that influence advertising customization).[109] New federal legislation would mandate this protection, as well as require companies to meet the other provisions of the statute.

While onerous, inflexible federal legislation should be rejected, Congress should enact a comprehensive federal statute regulating the collection of personal data by companies. Without new legislation, users are left to rely on piecemeal regulation and privacy policies that could change on a daily basis. Some have deemed this to be the "Information Age economy." The Information Age clearly has brought many benefits, as its technology has rapidly advanced, but the relevant law has failed to keep pace.

투고일 2010. 11. 16 심사완료일 2010. 12. 3 게재확정일 2010. 12. 7

109) Interview with Anne Toth, head of privacy at Yahoo, on C-Span (Sept. 18, 2010), available at http://www.c-span.org/Watch/Media/2010/09/18/COM/A/38187/Anne+Toth+Yahoo+Policy+Vice+President++Head+of+Privacy.aspx.

References

Restatement (Second) of Torts §§652B, 652C, 652D, 652E (1977).

Daniel J. Solove & Paul M. Schwartz, Information Privacy Law, (3d ed. 2009).

Valentine v. NebuAd, No. 08 Civ. 5113 (N.D. Cal. Nov. 10, 2008).

In re DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

Dyer v. Northwest Airlines Corp. 334 F.Supp.2d 1196 (D.N.D. 2004).

In re Pharmatrak, Inc. Privacy Litigation, 220 F.Supp.2d 4, 13 (D.Mass. 2002).

In re Northwest Airlines Privacy Litigation, 2004 WL 1278459 (D. Minn. 2004).

Federal Trade Commission v. Seismic Entertainment Productions, Inc., Civ. No. 1:04-CV-00377 (Nov. 21, 2006)

In re Liberty Financial Cos., No. 9823522, 1999 FTC LEXIS 99 (May 6, 1999)

FTC v. ReverseAuction.com, Inc., No. 00-CV-32 (D.D.C. Jan. 6, 2000)

In re Gateway Learning Corp., No. C-4120 (Sept. 10, 2004).

FTC v. Toysmart.com LLC, 00-CV-11341-RGS (D. Mass. July 10, 2000).

U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989).

Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

Children's Online Privacy Protection Act (1998), 15 U.S.C.A. §§6502-6505.

Videotape Privacy Protection Act of 1988, 18 U.S.C. §2710 (2000).

The Cable Communications Policy Act, 47 U.S.C. §551 et seq (2003).

Electronic Communications Privacy Act (1986), 18 U.S.C. §2510.

Computer Fraud and Abuse Act (1986), as codified at 18 U.S.C. §1030.

Telephone Consumer Protections Act (1991), 47 U.S.C. §227.

CAN-SPAM Act (2003), 15 U.S.C.A. §§7701, et seq.

The Federal Trade Commission Act (1914) (15 U.S.C §§41-58, as amended).

Minnesota's Deceptive Trade Practices Act, Minn.. Stat. §325D.44.

Financial Services Modernization Act, Pub. L. No. 106-102, codified at 15 U.S.C. §§6801-6809.

Daniel J. Solove, *Conceptualizing Privacy*, 90 Cal .L. Rev. 1087 (2002).

Louise Story and Miguel Helft, *Google Buys DoubleClick for $3.1 Billion*, The New York Times, April 14, 2007.

Julia Angwin, *The Web's New Gold Mine : Your Secrets*, The Wall Street Journal, July 30, 2010.

Ryan Singel, *Today Facebook, Tomorrow the World*, Wired, Apr. 23, 2010, available at http://www.wired.com/epicenter/2010/04/facebook-becomes-web/comment-page-1.

Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 Hastings L.J. 1227, 1251 (2003).

Tresa Baldas, *Web Behavioral Advertising Goes to Court*, The National Law Journal, March 2, 2009, available at http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202428691751.

Liisa M. Thomas and Monique N. Bhargava, *Where Have You Been? The Rules for Online Behavioral Advertising*, Pratt Privacy & Data Security Law Journal, September 2009.

Jeff Sovern, *Protecting Privacy with Deceptive Trade Practices Legislation*, 69 Fordham L. Rev. 1305, 1352-53 (2001).

Joel R. Reidenberg, *Privacy in the Information Economy : A Fortress or Frontier for Individual Rights?*, 44 Fed. Comm L.J. 195, 208 (1992).

William M. Beaney, *The Right to Privacy and American Law*, 31 L. & Contemp. Probs. 253, 255 (1966).

Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 198 (1890).

Nick Bilton, *Consumer Group Aims at Google*, The New York Times, September 6, 2010.

Julie E. Cohen, *Examined Lives: Informational Privacy and The subject as Object*, 52 Stan.L.Rev. 1373 (2000).

Jonathan Shaw, *Exposed, The erosion of privacy in the Internet era*, Harvard Magazine, September October 2009, at http://harvardmagazine.com/2009/09/privacy-erosion-in-internet-era.

Charles Dunigg, *What Does Your Credit-Card Company Know about You?*, The New York Times, May 12, 2009.

See Nancy J. King, *When Mobile Phones Are RFID-Equipped-Finding E.U.-U.S. Solutions to Protect Consumer Privacy and Facilitate Mobile Commerce*, 15 Mich. Telecomm. Tech. L. Rev. 107, 145 (2008).

Michael Barbaro and Tom Zeller Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, The New York Times, Aug. 9, 2006.

Emily Steel and Julia Angwin, *On the Web's Cutting Edge, Anonymity in Name Only*, The Wall Street Journal, August 4, 2010.

Kevin Bankston, *Facebook's New Privacy Changes : The Good, The Bad, and The Ugly*, December 9, 2009, at http://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly

Anita L. Allen, *Coercing Privacy*, 40 Wm. & Mary L.Rev. 723 (1999).

Eric Goldman, *The Privacy Hoax*, Forbes (Oct. 14, 2002).

Tanzina Vega, *Web Code Offers New Ways To See What Users Do Online*, The New York Times, October 11, 2010.

Daniel J. Solove, *Privacy and Power : Computer Databases and Metaphors for Information Privacy*, 53 Stan.L.Rev. 1393, 1452 (2001).

Elizabeth Warren, *Unsafe at Any Rate*, Democracy Journal, Issue #5, Summer 2007.

Tanzina Vega, *Code That Tracks Users' Browsing Prompts Lawsuits*, The New York Times, September 21, 2010.

Riva Richmond, *Resisting the Online Tracking Programs*, New York Times, November 11, 2010.

Riva Richmond, *False Sense of Security*, The New York Times, September 20, 2010

States to Investigate Google Data Collection, Reuters, June 21, 2010.

AJ Glasser, *Zynga gave advertisers user info*, The Wall Street Journal, October 18, 2010.

Sarah Ludington, *Reining in the Data Traders : A Tort for the Misuse of Personal Information*, 66 Md. L. Rev. 140 (2007).

Steven A. Hetcher, *Norms in a Wired World* (2004).

Steven Hetcher, *Changing the Social Meaning of Privacy in Cyberspace*, 15 Harv. J. L. & Tech. 149 (2001).

Steven A. Hetcher, *Norm Proselytizers Create a Privacy Entitlement in Cyberspace*,

16 Berkeley Tech. L. J. 877 (2001).

Priscilla M. Regan, *Legislating Privacy* : Technology, Social Values, and Public Policy (1995).

Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry doesn't Get)*, 2001 Stan. Tech. L. Rev. 1.

Michael E. Staten & Fred H. Cate, *The Impact of Opt-In Privacy Rules on Retail Credit Markets : A Case Study of MBNA*, 52 Duke L.J. 745 (2003).

Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley & Michael Hennessy, Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities That Enable It (2009).

Internet World Stats, Usage and Population Statistics, http://www.internetworldstats.com/am/us.htm (last visited Nov. 14 2010).

http://dealbook.nytimes.com/2010/01/06/apple-buys-quattro-an-ad-firm/

Fed. Trade Comm'n, FTC Policy Statement on Deception (1983), available at http://www.ftc.gov/bcp/policystmt/ad-decept.htm.

Prepared Statement of the Federal Trade Commission On Consumer Privacy, Presented By Chairman Jon Leibowitz Before the Committee on Commerce, Science, and Transportation, United States Senate (July 27, 2010), at http://www.ftc.gov/os/testimony/100727consumerprivacy.pdf.

http://www.clickz.com/clickz/news/1700857/doubleclick-settles-states-on-profiling

National Conference of State Legislatures, State Security Breach Notification Laws, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm (last visited Nov. 14, 2010) (listing the notification laws).

http://www.facebook.com/policy.php

http://news.smh.com.au/breaking-news-technology/facebook-finds-apps-giving-user-id-data-to-advertisers-20101019-16r2c.html

http://www.techi.com/2010/06/the-dark-side-of-technology/.

Symantec 2010 State of Enterprise Security Study Shows Frequent, Effective Attacks on Worldwide Business, available at http://www.symantec.com/about/news/release/article.jsp?prid=20100221_01.

Scott Cleland, Americans want online privacy − per new Zogby poll, June 8, 2010,

available at http://precursorblog.com/content/americans-want-online-privacy-new-zogby-poll

http://www.cdt.org/privacy/guide/surveyinfo.php

Most Americans dislike behavioral advertising: survey, September 30, 2009, available at http://www.physorg.com/news173555711.html

Available at http://www.socialtimes.com/2010/10/government-policy-on-internet-privacy/

Pew Internet and American Life Project, Teens, Privacy, and Online Social Networks, available at http://www.pewinternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx?r=1.

http://www.businesswire.com/news/home/20100720005040/en/Facebook-Flops-ACSI-E-Business-Report

http://www.cdt.org/privacy/guide/surveyinfo.php

Danny Sullivan, Dear Facebook & Google: We Are Not Your Pawns Enough With The Auto Opt-In!, Daggle, April 23, 2010, available at http://daggle.com/dear-facebook-google-pawns-optin-1796

News release, FTC. ChoicePoint Settles Data Security Breach Charges (Jan. 26, 2006), available at http://www.ftc.gov/opa/2006/01/choicepoint.htm.

Joseph Turow, Annenberg Pub. Policy Ctr. of the Univ. of Pa., Americans and Online Privacy: The System Is Broken (2003), available at http:// www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf

Interview with Rick Boucher and Cliff Stearns, on C-Span, the Communicators, (Oct. 2, 2010) [hereinafter C-Span interview), available at http://www.c span.org/Watch/Media/2010/10/02/HP/A/38840/Reps+Rick+Boucher+DVA+and+Cliff+Stearns+RFL.aspx.

Interview with Anne Toth, head of privacy at Yahoo, on C-Span (Sept. 18, 2010), available at http://www.c-span.org/Watch/Media/2010/09/18/COM/A/38187/Anne+Toth+Yahoo+Policy+Vice+President++Head+of+Privacy.aspx.

Liisa M. Thomas, Balancing Technology and Power: Emerging Rules in Online Behavioral Advertising, Mobile Marketing, Social Networking, and Other Electronic Commercial Communications, Presentation at PLI's Eleventh Annual Institute on Privacy and Data Security Law, Chicago (July 2010).

Regulatory Restructuring : Enhancing Consumer Financial Products Regulation: Statement Before the H. Comm. on Financial Servs., 111th Cong. (2009) (statement of Elizabeth Warren).