NOTE

SELECTIVE PRIVACY: FACILITATING MARKET-BASED SOLUTIONS TO DATA BREACHES BY STANDARDIZING INTERNET PRIVACY POLICIES

*Karim Z. Oussayef**

TABLE OF CONTENTS

I. INTRODUCTION: AMERICA ONLINE

On August 6th 2006, several blogs noticed that America Online's ("AOL") research site contained an archive file called 500kusers.tgz.[1] The massive file included a "readme",[2] apparently from AOL's research department, which explained that it contained the search terms of more than 600,000 users from March to May of 2006.[3] The file did not identify users by name.[4] However, it

* J.D. Candidate Boston University School of Law 2008; B.S., cum laude, with High Distinction in Computer Science, University of Rochester, May 2004. I would like to thank professor Dennis Crouch for comments and suggestions.

[1] See Michael Arrington, AOL Proudly Releases Massive Amount of Private Data, TECHCRUNCH, Aug 7, 2006, http://www.techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data.

[2] A readme is a small text file that describes included software or data.

[3] See AOL's original description, http://www.gregsadetsky.com/aol-data/U500k_README.txt (last visited Nov. 17, 2006).

linked each query with a unique user number, and searches often contained identifying information such as nearby addresses and the names of family members.[5] Many commentators hypothesized that the file contained enough information to link individuals to their user number.[6] The New York Times eventually confirmed this theory by tracking down and interviewing one of AOL's customers.[7]

AOL subsequently admitted in blog posts[8] and press releases[9] that they inadvertently exposed the information. According to AOL, "it was an innocent enough attempt to reach out to the academic community with new research tools, but it was obviously not appropriately vetted, and if it had been, it would have been stopped in an instant."[10] AOL quickly took down the original link to the file, but the information was still available on Google Cache for several days.[11] Many people accessed the information during that time,[12] and the data are still available from several websites.[13]

The AOL incident is just one of several recent privacy breaches.[14] However, the scope of AOL's disclosure is especially troubling. It represents the private information of more than a half-million people and about 1.5% of

[4] *See id.*

[5] *See* Philipp Lenssen, *AOL Shared Private Search Queries*, GOOGLE BLOGOSCOPED (Aug. 7, 2006), http://blog.outer-court.com/archive/2006-08-07-n22.html.

[6] *E.g., id.*

[7] Michael Barbaro & Tom Zeller Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N. Y. TIMES, Aug. 9, 2006, at A1.

[8] *See e.g.,* Michael Arrington, *AOL: "This was a screw up"*, TECHCRUNCH (Aug. 7, 2006), http://www.techcrunch.com/2006/08/07/aol-this-was-a-screw-up.

[9] Press Release, America Online, AOL apologizes for releasing search log data (Aug. 7, 2006); *see also* Dawn Kawamoto and Elinor Mills, *AOL apologizes for release of user search data*, CNET NEWS.COM (Aug. 7, 2006), http://news.com.com/2100-1030_3-6102793.html.

[10] Arrington, *supra* note 8.

[11] *See* Arrington, *supra* note 8. Google Cache is a Google service which archives and allows Internet searchers to access older versions of a website. *See* Google Help Center, http://www.google.com/help/features.html#cached (last visited Jan. 13, 2007).

[12] *See e.g.* Lenssen, *supra* note 5.

[13] *E.g.* Greg Sadetsky, *AOL Search Data Mirrors*, http://www.gregsadetsky.com/aol-data (last visited Jan. 14, 2007); AOL Search Database, http://www.aolsearchdatabase.com (last visited Apr. 2, 2007). Although I hesitate to give further access to private information, the data are already available from several websites.

[14] The Privacy Rights Clearinghouse provides a list of recent security breaches. Privacy Rights Clearinghouse, *A Chronology of Data Breaches* (2007), http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Jan. 13, 2007). An interested reader can signup for email updates on various privacy breaches. Attrition.org Data Loss Archive and Database, http://attrition.org/dataloss (last visited Jan. 13, 2007). I receive one or two emails a day notifying me of recent privacy breaches.

AOL's May search queries.[15] Furthermore, the information is available to the public. In many privacy breaches, the disclosure remains fairly contained. For example, in some cases, companies only expose information to a particular person or organization.[16] In other cases, companies lose computer hardware and privacy concerns remain speculative.[17] The AOL case, in contrast, allows anyone with an Internet connection to access the search queries. One website even organizes the information in a user-friendly interface.[18]

Casual Internet surfers can use (or misuse) the information in ways that seriously threaten the privacy of the affected AOL subscribers. User 18471744 provides a good example of the implications of AOL's disclosure.[19] His or her search terms include "texas [sic] laws on retirement plans", "legal separation", and "is a restraining order needed during a divorce."[20] From this information we might assume that this user is considering divorce. An unscrupulous person could use this information to embarrass or even blackmail the individual. Despite the personal nature of user 18471744's queries, this information is relatively tame compared to other searches.[21] Commentators have discovered queries aimed at finding lost relatives, cheating on a significant other, and viewing child pornography.[22] Some of these searches include full names or other identifying information.[23]

Against the backdrop of AOL's disclosure, this note examines the legal and economic factors that contribute to privacy breaches. Part I analyzes common methods of obtaining private information. It explains how search engines, cookies, and voluntary exchanges of personal information allow companies to accumulate detailed information about their visitors. Part II examines other recent privacy breaches—such as those resulting from intentional disclosure, legal discovery, and security flaws—and tries to identify common circumstances that contribute to their occurrence. Part III examines regulations that attempt to protect online privacy. It argues that the current system of

[15] Sadetsky, *supra* note 13.

[16] Here, for example, AOL was presumably attempting to release the information to small group of researchers. *See* AOL's Original Description, *supra* note 3.

[17] *See* Martin H. Bosworth, *VA Loses Data on 26 Million Veterans*, CONSUMERAFFAIRS.COM, May 22, 2006, http://www.consumeraffairs.com/news04/2006/05/va_laptop.html (last visited Feb. 15, 2007) ("In every public case, company representatives insist the laptops are stolen simply for their resale value, as opposed to the data they contain.").

[18] AOL Search Database, *supra* note 13.

[19] In the interest of preventing further exposure of private information, I have selected a user whose search terms do not include proper names, addresses, or other identifying information. Note that many of the search terms do include such information.

[20] Sadetsky, *supra* note 13.

[21] Lenssen, *supra* note 5 (providing examples of embarrassing, illegal, and private queries).

[22] Lenssen, *supra* note 5.

[23] Lenssen, *supra* note 5.

sector-specific Federal legislation relies on a self-regulatory philosophy. As a result, most companies that collect private information are not required to comply with meaningful safeguards. Part III also explains how privacy policies attempt to compensate for legislative shortcomings. Part IV explains the limitations of privacy policies in the *status quo*. It discusses how complex language, lack of meaningful choice, and weak enforcement mechanisms prevent privacy policies from being effective. Finally, Part V suggests that through limited regulation, Congress could make privacy policies much more effective. Companies should choose from a limited set of government-standardized privacy policies instead of creating their own. This proposal would help companies implement their policies in a way that benefits reasonably alert consumers and responsible data collectors alike.

II. PART I: DATA COLLECTION

Companies first recognized the importance of collecting information about their customers long before the advent of the Internet.[24] Companies initially collected customer information to increase the efficiency of direct marketing campaigns.[25] The government helped marketing companies categorize their customers when it started using zip codes and selling census information in the 1960s and 70s.[26] Customers are now accustomed to questions about their phone number, zip code, or even income when making routine purchases at clothing retailers or shopping malls.[27] However, collecting and aggregating this information offline is inefficient, and consumers can always refuse to give out personal information.[28] In contrast, electronic communication allows for automated data collection. It requires little effort or cost to collect information from website visitors.[29] Since information already passes through servers when Internet browsers request information, website administrators can choose

[24] *See* James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 17 (2003).

[25] *See id.*

[26] *See id.*

[27] Merchants are starting to use tactics that are similar to online data collection. *See* Chris J. Hoofnagle, *Privacy Self Regulation: A Decade of Disappointment*, March 4, 2005, http://www.epic.org/reports/decadedisappoint.html (discussing practices such as asking for customer phone numbers, encouraging grocery and pharmacy loyalty cards, and managing customer return databases).

[28] *See* Clifford S. Fishman, *Technology and the Internet: The Impending Destruction of Privacy by Betrayers, Grudgers, Snoops, Spammers, Corporations, and the Media*, 72 GEO. WASH. L. REV. 1503, 1511 (2004); Nehf, *supra* note 24, at 17.

[29] Several companies offer website analytic services. *E.g.* Nielsen//NetRatings, http://www.nielsen-netratings.com (last Apr. 2, 2007); My Site Traffic, http://www.mysitetraffic.com (last visited Apr. 2, 2007); Boxes and Arrows, http://www.boxesandarrows.com (last visited Apr. 2, 2007); Site Meter, http://www.sitemeter.com/default.asp (last visited Apr. 2, 2007).

to log the information.[30] Once a website implements the appropriate code, it can continue to collect information without additional effort.[31]

Large-scale data collection can help Internet companies improve their services. For example, websites can use information about their visitors to better tailor information to a particular market.[32] Companies can also optimize server performance by predicting how many users will visit the site at a particular time.[33] Consumers are the beneficiaries of many of these advantages. However, the extent of private information, spread across many self-regulated databases, raises privacy concerns.[34] What follows is a brief survey of how Internet companies collect personal information.

Search engines account for an enormous proportion of website visits,[35] and most search engines keep track of users' search queries.[36] AOL's disclosure of its users' search queries was particularly significant because people often use AOL both as an internet service provider ("ISP") and a search engine. When customers use their ISP's search engine their queries can be linked to a unique identifier.[37] In the case of AOL's data breach, the data file categorized the search data by user instead of listing the searches sequentially. This practice allowed third parties to accumulate information from several queries and associate it with a single user.[38] In contrast, if customers do not use their ISP's

[30] *See* Fran Diamond, *Web Traffic Analytics and User Experience*, BOXES AND ARROWS, July 28, 2003, http://www.boxesandarrows.com/view/web_traffic_analytics_and_user_experience.

[31] *See* Fishman, *supra* note 28, at 1533-34 (discussing the use of cookies).

[32] *See* Diamond, *supra* note 30.

[33] *See* Larry Becker, *Three Analytics You'll Meet in 2.0*, MULTICHANNEL MERCHANT, October 1, 2007 at 32; Diamond, *supra* note 30.

[34] *See* Fishman, *supra* note 28, at 1511 ("[T]here is no central depository where all of this information is kept. . . . [C]ontrollers of these databases are restrained only by promises not to reveal the information and fear of adverse publicity if they do share it.").

[35] Alexa ranks websites by page views and reach (number of users). According to the January rankings, the four most popular sites were all search engines: Yahoo!, MSN, Google, and Baidu. Alexa, http://www.alexa.com (last visited Jan. 28, 2007).

[36] *See* Wall Street Journal Online, *Should Web Search Data Be Stored?*, August 15, 2006, http://online.wsj.com/public/article/SB115530662685133335-OJwdGqVy4BFV8l10JmjhOxqaoHc_ 20060913.html.

[37] *See* Electronic Frontier Foundation, *Six Tips to Protect Your Online Search Privacy*, http://w2..eff.org/Privacy/search/searchtips.pdf (last visited Nov. 18, 2006).

[38] *See* Lenssen, *supra* note 5 ("What's really interesting is that **queries were connected to a user ID**. . . and there goes your privacy. Based on a sequence of searches it is often trivial to connect a person to a user ID. For example, user 500 may search for "link:mysite.com", and then user 500 may search for the name 'John Doe.' Now you can verify that mysite.com's webmaster is John Doe from San Francisco, and you have a good indicator that user 500 is indeed John Doe. Finally, you look at other queries from this user – like, 'jobs San Francisco' – and you have strong indicators that John Doe is looking for a job behind his current boss's back.") (emphasis and ellipsis in original).

search engine, their Internet Protocol ("IP") addresses leave a less precise trail.[39] Although information from IPs is more difficult to link to a particular user, it may still allow search engines to link queries to particular users.[40] Linking IP addresses to Internet users is becoming easier as more users are switching to digital subscriber lines ("DSL") or cable modems.[41] Most Internet browsers warn users that third parties could intercept and read the information they submit, but few users pay attention to these warnings.[42]

Cookies are another tool for collecting personal information. Cookies are small text files that web servers store on connecting computers.[43] They identify visitors by associating computers with unique IDs.[44] Every time visitors return to a website, the server can read their text files and match the ID to any information that the website has collected about them.[45] In this way, the website can "recognize" a particular computer and personalize information to that user.[46] Cookies are extremely useful to website visitors. They allow visitors to use online shopping carts, automatically log in to websites, and customize services to their needs.[47] However, cookies also benefit website operators and may work against the visitor's interests. Many websites use cookies to tailor advertisements to particular consumers.[48] For example, if you purchase a book about cars, the site might link your cookie with your purchase. The next time you visit the site, the server could read your cookie and communicate your ID to the website. From then on, the website might show

[39] *See* Federal Trade Commission, *Privacy Online: A Report to Congress, Part 2 Recommendations* (July 2000) n.14, http://www.ftc.gov/os/2000/07/onlineprofiling.pdf. An IP address is a unique number that allows devices to communicate with each other; *See id.*

[40] *See* Federal Trade Commission, *supra* note 39.

[41] Dialup ISPs change the IP address of their users each time they connect to the Internet. In contrast, cable modems assign semi-static IP addresses. As a result, a particular modem (and thus computer) keeps the same address for a longer amount of time. This would make it easier for a ISP to link search terms to a particular person. *See id.*

[42] When individuals use a browser for the first time, by default, it will warn them whenever they submit information through a web dialog. For example, Internet Explorer warns users "[w]hen you send information to the Internet, it might be possible for others to see that information. Do you want to continue?"

[43] David Goldman, *I Always Feel Like Someone is Watching Me: A Technological Solution for Online Privacy*, 28 HASTING COMM. & ENT. L.J. 353, 364 n.43 (2005-2006) (citing John Schwartz, *Giving Web a Memory Cost Its Users Privacy*, N.Y. TIMES, Sept. 4, 2001, at A1).

[44] *Id.*

[45] *Id.*

[46] *See id.*

[47] *See id.* The reader can surf the web without cookies by adjusting the privacy preferences of his or her browser. This quickly becomes aggravating as several useful website features become no longer available. Goldman, *supra* note 43.

[48] Brain Morrissey, *Reuters, Financial Times to Offer Target Ads*, DMNEWS, March 15th, 2004, http://www.dmnews.com/cms/dm-news/internet-marketing/26844.html.

you car advertisements instead of generic advertisements.[49] Depending on the success of the analysis and the visitor's interests, these targeted advertisements could be helpful, annoying, or ignored completely.

In many cases, users might want to intentionally give websites information to make the sites more informative or entertaining. Countless websites collect information in this way. For example, many online retailers encourage shoppers to create "wish lists" where they can add items that they would like to buy in the future.[50] Some websites allow users to create their own personalized radio station from information about their music preferences.[51] Many news sites require user registration to access articles or features.[52] Some websites offer incentives for filling out surveys or providing other marketing information.[53] Most Internet users seem willing to provide such information if they get something in return.[54] Many commentators overlook the privacy implications of voluntary data collection, perhaps because it seems too obvious or benign. However, even volunteered information can give rise to privacy concerns. Websites might use information in different ways than the user intended or might disclose the information to third parties. For example, visitors might provide their email address to receive product updates, only to receive frequent email advertisement as part of the deal. Similarly people might consciously supply their address to mapping websites, like MapQuest or Google Maps, and still expect the information to be confidential.

Companies use several other data collection methods that are beyond the scope of this note. New methods tend to concentrate on collecting information without explicit consent. Several commentators have discussed the implications of spyware,[55] webbugs,[56] and email content extraction.[57] As the

[49] *See* Fishman, *supra* note 28, at 1536 (discussing how DoubleClick's cookies targeted banner ads to particular consumers in In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 502-03 (S.D.N.Y. 2001)).

[50] *See e.g.* Amazon.com Help, http://www.amazon.com (follow the "help" hyperlink) (explaining shoppers' ability to create shopping lists, wish lists, baby registries, and wedding registries).

[51] *See e.g.* LastFM, http://last.fm (last visited Jan. 21, 2007); Pandora, http://www.pandora.com (last visited Jan. 21, 2007).

[52] For example, the New York Times online site requires free registration to access some articles. Registering for NYTimes.com, http://www.nytimes.com/regi (last visited Jan. 21, 2007). One website attempts to get around registration by sharing fake login names. BugMeNot, http://www.bugmenot.com (last visited Jan. 21, 2007).

[53] *See e.g.* MySurvey.com, http://www.mysurvey.com (last visited Jan. 21, 2007) (giving users money or rewards for participating in surveys); BzzAgent, http://www.bzzagent.com (last visited Jan. 21, 2007) (giving users free products in exchange for feedback).

[54] *See* Goldman, *supra* note 43, at 386 (suggesting that a technological solution to privacy issues that would, among other things, make it easier for consumers to share or sell their information).

[55] *E.g.* Jordan M. Blanke, *"Robust Notice" and "Informed Consent:" the Keys to Successful Spyware Legislation*, 7 COLUM. SCI. & TECH. L. REV. 2 (2006); Susan P.

Internet continues to mature, information gathering techniques will surely become even more sophisticated.[58]

III. PART II: DATA BREACHES

Although most Internet users have some privacy concerns when they use the Internet, many are unaware of the amount of information that companies collect.[59] This phenomenon helps explain why people feel comfortable betraying private thoughts to search engines that they might be reluctant to tell a close friend.[60] It might also explain why people occasionally behave with remarkable candor[61] and rudeness[62] when they communicate online. Not surprisingly, people who are aware of privacy issues are more reluctant to use the Internet.[63] This expectation of privacy puts a huge responsibility on companies that collect private data. However, data breaches continue to occur frequently. Examining how different types of privacy breaches occur will help identify the root causes and prevent future incidents. The next section describes three major categories of data breaches: intentional actions, legal

Crawford, Symposium, *Spyware: The Latest Cyber-Regulatory Challenge, First Do No Harm: The Problem of Spyware*, 20 Berkeley Tech. L.J. 1433 (2005).

[56] *E.g.* Stefanie Olsen, CNET News.com, *Web Bug Swarm Grows 500 Percent*, Aug. 14, 2001, http://news.com.com/2100-1023-271605.html; *see also* Electronic Frontier Foundation, *supra* note 37.

[57] *E.g.* Sarah Elton, *Got a Date Friday? Google Knows.* MACLEAN'S, Augest 28, 2006 at 5; Hoofnagle, *supra* note 27.

[58] *See* Electronic Frontier Foundation, *supra* note 37.

[59] *See generally* Beth Givens, *Symposium on Internet Privacy: Privacy Expectations in a High Tech World*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 347, 352 (2000).

[60] Again, the AOL search terms provide many examples of personal matters that most people would be reluctant to discuss in person.

[61] Several bloggers have stirred up controversy by criticizing their employers or disclosing inappropriate information. *E.g.* Evan Hansen, *Google Blogger Has Left the Building*, CNET NEWS.COM, Feb. 8, 2005, http://news.com.com/Google+blogger+has+left+the+building/2100-1038_3-5567863.html; Donald MacLeod, *Lecturer's Blog Speaks Free Speech Row*, GUARDIAN UNLIMITED, May 3, 2006, http://education.guardian.co.uk/higher/news/story/0,,1766663,00.html (where a lecturer blogged that "the academic staff are too busy with research to have their minds on teaching") .

[62] Anyone who has visited electronic message boards, blog comments, or chat rooms knows how quickly a civil conversation can devolve to ad hominem attacks. *See e.g.* Owen Gibson, *Warning to chat room users after libel award for man labeled a Nazi*, THE GAURDIAN, March 23, 2006, http://www.guardian.co.uk/law/story/0,,1737445,00.html (describing a British libel case where a woman insulted someone who criticized the Iraq war).

[63] Federal Trade Commission, *Privacy Online: A Report to Congress*, June 1998, at 3, available at http://www.ftc.gov/reports/privacy3/priv-23a.pdf (citing *Business Week/Harris Poll: Online Insecurity,* BUSINESS WEEK, March 16, 1998, at 102.).

discovery, and security breaches.

A. Intentional Actions

Toysmart is a notorious example of how some companies intentionally release private information. Toysmart was a successful online retailer that sold children's toys on the Internet.[64] Like many websites, Toysmart collected information about its customers "including name, address, billing information, shopping preferences, and family profiles-which included the names and birthdates of children."[65] Visitors voluntarily provided this information, encouraged by a privacy policy that promised never to share the information with third parties.[66] However, in June of 2000, Toysmart entered bankruptcy and attempted to sell its assets.[67] Toysmart also tried to sell its customer database in violation of its strict privacy policy.[68] When this decision became public, it drew criticism from several privacy advocates.[69] Eventually, the Federal Trade Commission ("FTC") intervened and filed suit in Federal court.[70] The FTC and Toysmart quickly settled, and Toysmart agreed not to sell their customer list except under restrictive circumstances.[71] This scenario is not an isolated event as other failing Internet companies have attempted to sell their customer data.[72]

---

[64] *See* L. Richard Fischer and Shannon K. Ryerson, *FTC Punishes Toysmart*, 1 PRIVACY & INFORMATION LAW REPORT 18 (2000).

[65] *Id.*

[66] One restriction stated: "personal information, voluntarily submitted by visitors to our site, such as name, address, billing information and shopping preferences, is never shared with a third party," and another stated: "when you register with toysmart.com, you can rest assured that your information will never be shared with a third party." Mark D. Robins, *How the FTC's Actions in Toysmart Shed Light on Two Key Privacy Issues*, 5 CYBERSPACE LAWYER NO. 7, at 6 (2000).

[67] *See id.*

[68] *See id.*

[69] *See* Patricia Jacobus, *Privacy Group Criticize New Amazon Policy*, CNET NEWS.COM, September 13, 2000, http://news.com.com/2100-1017-245676.html.

[70] See FTC v. Toysmart.com, LLC, Civil Action No. 00-11341-RGS, Complaint (D. Mass. 2000), available at http://www.ftc.gov/os/2000/07/toysmartcmp.htm.

[71] "The settlement only allows a sale of such lists as a package which includes the entire Web site, and only to a 'Qualified Buyer'— an entity that is in a related market and that expressly agrees to be Toysmart's successor-in-interest as to the customer information." Press Release, Federal Trade Commission, FTC Announces Settlement With Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations (July 21, 2000), available at http://www.ftc.gov/opa/2000/07/toysmart2.htm; *see also* F.T.C. v. Toysmart.com, LLC, Civil Action No. 00-11341-RGS, Stipulated Consent Agreement and Final Order (D. Mass 2006), available at http://www.ftc.gov/os/2000/07/toysmartconsent.htm.

[72] *See* Greg Sandoval, *Failed dot-coms May Be Selling Your Privacy Information*, CNET NEWS.COM, June 29, 2000, http://news.com.com/2100-1017-242649.html; Greg Sandoval,

B. Legal discovery

Companies might also disclose private information pursuant to a the legal process. In a lawsuit that continues to raise privacy issues, the American Civil Liberties Union ("ACLU") sued to prevent enforcement of the Child Online Protection Act ("COPA").[73] COPA[74] attempts to protect children from "material harmful to children" on the Internet.[75] The ACLU argued, *inter alia*, that COPA was overly broad and prevented adult freedom of expression.[76] The case ended up reaching the Supreme Court twice.[77] On its second review of the case, the Supreme Court determined that the law was likely overbroad and remanded to determine if there were less restrictive ways of protecting children.[78] As a result, the Department of Justice ("DOJ") had the burden of showing that "COPA is the least restrictive alternative available to accomplish Congress' goal".[79] In an attempt to prove the technological feasibility of COPA, the DOJ subpoenaed records from several search engines including Google.[80] The DOJ asked for billions of sample URLs,[81] and all search queries from the past two months.[82] By analyzing this data, the DOJ hoped to "'measure the effectiveness of content filters' that attempt to screen sexually explicit material from minors,"[83] and prove that COPA was narrowly tailored.

eTour Accused of Selling Customer Info, CNET NEWS.COM, May 25, 2001, http://news.com.com/eTour+accused+of+selling+customer+info/2100-1023_3-258344.html.

[73] ACLU v. Reno, 1998 U.S. Dist. LEXIS 18546 (D. Pa. 1998). Note that there is significant subsequent history that this note does not discuss.

[74] *See* 47 U.S.C. § 231 (2006). Note that the Child Online Protection Act (COPA) is distinct from the Children's Online Privacy and Protection Act (COPPA), discussed *infra*.

[75] *Id.*

[76] ACLU v. Janet Reno, Civil Action No. 98-CV-5591, Complaint (E.D. PA. 1998), available at http://www.epic.org/free_speech/copa/complaint.html.

[77] ACLU v. Reno, 542 U.S. 656 (2004); ACLU v. Reno, 535 U.S. 564 (2002).

[78] *See* ACLU v. Reno, 542 U.S. at 673.

[79] *Id.*

[80] *See* Michael Hiltzik, *Vague U.S. Statute Underlies Google Case*, LOS ANGELES TIMES, March 27, 2006 at C1.

[81] A URL, or Uniform Resource Locator, is a website address. In effect, the government was asking for all the websites in Google's search database. *See id.* Since Google's search engine attempts to catalog all websites on the Internet, this was tantamount to asking for the address of every website on the Internet. *See* Sergey Brin and Lawrence Page, *The Anatomy of a Large-Scale Hypertextual Web Search Engine*, 30 COMPUTER NETWORK 107 (1998), available at http://infolab.stanford.edu/~backrub/google.html (describing how Google and other search engines catalog web pages).

[82] *See* Hiltzik, *supra* note 80.

[83] Judge Grants Subpoena For Google URLs But Not Search Queries, 8-1 Mealey's Litig. Rep. Cyber Tech & E-Com. 8 (2006) (quoting the Department of Justice).

Google was the only search engine that challenged the subpoena.[84] It cited concerns of losing customer goodwill and the potential disclosure of trade secrets.[85] The DOJ responded by reducing its request to 50,000 sample URLs and 5,000 search queries.[86] The district court analyzed the DOJ's modified request pursuant to the Federal Rules of Civil Procedure.[87] It balanced the broad scope of Rule 26(b), which allows parties to discover evidence "relevant to the claim or defense of any party," against the restrictions imposed by Rule 26(b)(2)(c)(iii), which prevents discovery methods where "the burden or expense of the proposed discovery outweighs its likely benefit."[88] The court concluded that both the sample URLs and the search queries were relevant to the government's case.[89] It thus permitted the DOJ to discover a sample of Google's URLs.[90] However, the court was reluctant to release Google's search queries for several reasons. First, the court found that Google might lose goodwill by disclosing the personal information of its customers.[91] Second, Google persuaded the court that releasing search queries might allow competitors to reverse engineer Google's search indexing methods.[92] Although the court found that the current subpoena would not, by itself, disclose any secrets, it found that Google might become entangled in future litigation and broader discovery requests.[93] As a result of these concerns, the court denied the DOJ's motion to obtain user search queries.[94] Finally, in dictum, the court implied that third-party privacy issues might restrict subpoenas in similar situations.[95]

---

[84] *See id.*

[85] *See id.*

[86] *See id.* Note that the DOJ originally requested data which was very similar to what AOL disclosed on its website but on a larger scale. AOL only disclosed 1.5% of the queries that users had entered during a three month period; the DOJ subpoenaed all queries in a two month period. Also, note that Google receives significantly more search queries than AOL. *See* Alexis *supra*, note 35.

[87] *See generally* Gonzales v. Google, Inc., 234 F.R.D. 674 (D. Cal. 2006).

[88] *Id.* at 679-80 (citing Fed. R. Civ. P. 26(b)(1); Fed. R. Civ. P. 26(b)(2)(c)(iii)).

[89] Gonzales, 234 F.R.D. at 681-82.

[90] *See id.* at 688.

[91] *See id.* at 684 ("The expectation of privacy by some Google users may not be reasonable, but may nonetheless have an appreciable impact on the way in which Google is perceived, and consequently the frequency with which users use Google.").

[92] *See id.*

[93] *See id.* at 685.

[94] *See id.* at 688.

[95] Gonzales, 234 F.R.D. at 687. ("A user's search for '[user name] third trimester abortion san jose,' may raise certain privacy issues as of yet unaddressed by the parties' papers. This concern, combined with the prevalence of Internet searches for sexually explicit material generally not information that anyone wishes to reveal publicly—gives this Court pause.") This analysis was particularly astute because it predated AOL's privacy breach.

The use of subpoenas to access private information has become more widespread under the Digital Millennium Copyright Act ("DMCA").[96] Section 512(h) explicitly allows copyright owners to subpoena the ISPs of users who might be infringing on their intellectual property.[97] For example, the Recording Industry Association of America ("RIAA") and Magnolia Pictures have used this provision to bring suit against suspected copyright infringers. [98] Privacy advocates have decried the increasing use of subpoenas to identify alleged infringers.[99] They point to instances of mistaken identity and use of the subpoena power to suppress free speech and fair use.[100] In these situations, copyright owners invade an innocent person's privacy without justification.[101] On the other hand, copyright owners rely on the DMCA's subpoena powers to protect their property, especially since digital technology makes copying (and pirating) easy and inexpensive.[102]

The increasing importance of ISP subpoenas sets the stage for future legal battles.[103] One problem with non-party subpoenas is that companies have little incentive to resist them.[104] Even strong privacy policies may include provisions to allow for the disclosure of subpoenaed information.[105] Google's arguments not-withstanding, companies suffer little harm by disclosing private information. They can always claim that they had to comply with the law. Usually, it is not worth risking liability or legal expenses by resisting subpoenas.[106] An effective solution to privacy breaches will need to balance the interests of legal discovery with privacy interests.

---

[96] *See* Sonia K. Katyal, *The New Surveillance*, 54 CASE W. RES. L. REV. 297, 335 (2003). (discussing the Recording Industry Association of America's use of the DMCA subpoena powers); 17 U.S.C. § 512(h) (2000).

[97] 17 U.S.C. § 512(h) (2000).

[98] *See* Katyal, *supra* note 96 at 335; Declan McCullagh, *Magnolia Pictures sends DMCA subpoena to Google, YouTube*, CNET NEW.COM, Mar. 7, 2007, http://news.com.com/2061-10796_3-6165269.html.

[99] *See e.g.* ELEC. FRONTIER FOUND., *UNSAFE HARBORS: ABUSIVE DMCA SUBPOENAS AND TAKEDOWN DEMANDS* (2003) http://www.eff.org/IP/P2P/20030926_unsafe_harbors.php.

[100] *See id.*

[101] *See* Katyal, *supra* note 96, at 370-75.

[102] ROBERT P. MERGES ET AL., INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE at 564-65 (4th ed. 2006).

[103] *See* Fred von Lohmann, *Could Future Subpoenas Tie You to 'Britney Spears Nude'?*, LAW.COM, February 6, 2006, http://www.law.com/jsp/article.jsp?id=1138961111185.

[104] *Cf.* Katyal, *supra* note 96, at 367 (arguing that faced with liability, the ISP might err on the side of the copyright owners and against the service subscriber).

[105] *See* von Lohmann, *supra* note 103.

[106] Katyal, *supra* note 96, at 367.

C. Security Failures

Security failures may be the most common cause of privacy breaches.[107] Maintaining proper security practices is difficult because would-be identity thieves constantly develop new tactics for obtaining private data. For example, hackers recently broke into one of AT&T's computer systems and accessed records of customers who had purchased DSL equipment through AT&T's online store.[108] However, obtaining this information was simply the first step in the hackers' complex plot.[109] They subsequently used the data in a phishing scheme.[110] By including some of the stolen information in emails to AT&T customers, the hackers tried gain the trust of their victims to obtain additional information.[111] The extent of the scheme did not appear in AT&T's press release,[112] and was only available to the public after journalists investigated internal company records.[113] Companies that control private information struggle to keep up with increasingly sophisticated security threats. In fact, an AT&T spokesperson admitted "we haven't seen anything like this before."[114]

The phishing scheme used by the AT&T hackers is an example of social engineering. This practice involves taking advantage of human psychology to gain access to secure non-public information.[115] In the AT&T case, the hacker used social engineering after they had already obtained some personal information. However, identity thieves can also target companies directly. Many companies that have excellent physical and technological security fall victim to social engineering.[116]

One of the most notorious examples of social engineering involved the 2005 data breach at ChoicePoint. ChoicePoint originally specialized in providing credit data to the insurance industry but it quickly acquired many other

[107] *See* Privacy Rights Clearinghouse, *supra* note 14 (listing recent privacy breaches).

[108] *See* Press Release, AT&T, AT&T Offers Credit Monitoring Service to Customers Whose Credit Cards Were Accessed (Aug. 29, 2006), http://www.att.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=22531.

[109] *See* David Lazarus, *Phishing Expedition at Heart of AT&T Hacking,* S.F. CHRON. Sept. 1, 2006, at D1.

[110] *See id.* The Anti-Phishing Work Group defines phishing as "schemes [that] use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. [By] [h]ijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond." Anti-Phishing Working Group, http://www.antiphishing.org (last visited Jan. 23, 2007).

[111] *See* Lazarus, *supra* note 109.

[112] *See* Press Release, AT&T, *supra* note 108.

[113] *See* Lazarus, *supra* note 109.

[114] Lazarus, *supra* note 109.

[115] *See generally* KEVIN D. MITNICK & WILLIAM L. SIMON, THE ART OF DECEPTION: CONTROLLING THE HUMAN ELEMENT OF SECURITY (2002).

[116] *See id.* at 3.

companies to become an all-purpose information broker.[117] ChoicePoint uses public records[118] about individuals as a starting point and augments them with credit history, conviction records, insurance claims, media reports, private investigations, and social security numbers.[119] The database now contains information about nearly every adult American citizen.[120] ChoicePoint sells the information to many private companies.[121] For example, companies often hire ChoicePoint to conduct background checks on potential employees.[122] ChoicePoint also has several contracts with the government, including law enforcement agencies[123] and election officials.[124]

In February of 2005, thieves posed as legitimate business customers by setting up false companies to obtain private information from ChoicePoint's database.[125] According to ChoicePoint's March 2005 8-K filing, the thieves were able to access the names, addresses, social security numbers, driver's license numbers, credit reports, and legal judgments of up to 145,000 people.[126] Many commentators attributed the data breach not to cunning social engineering, but to lax security standards and ignored warning signs.[127] The FTC eventually filed suit against ChoicePoint for making false and misleading statements about its privacy policies, violating the Fair Credit Reporting Act ("FCRA"), and engaging in unfair commercial practices.[128] The case settled in

[117] *See* Robert O'Harrow Jr., *In Age of Security, Firm Mines Wealth of Personal Data*, WASHINGTON POST, Jan. 20, 2005 , at A01.

[118] Public records often contain information that seems private. ChoicePoint collected records like "birth dates, driver's license numbers, license plate numbers, spouse names, maiden names, addresses . . . and the purchase price of every parcel of property a person has ever owned." Gary Rivlin, *Keeping Your Enemies Close*, N. Y. TIMES, Nov. 12, 2006, § 3, at 1.

[119] *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 169 (2004); Liz Pulliam Weston, *Insurers Keep a Secret History*, MSN, http://articles.moneycentral.msn.com/Insurance/InsureYourHome/InsurersKeepASecretHistoryOfYourHome.aspx (last visited Jan. 23 2007).

[120] Daniel Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 371 (2006).

[121] Rivlin, *supra* note 118.

[122] Kim Zetter, *ChoicePoint's Checks Under Fire*, WIRED NEWS, Mar. 23, 2005, http://www.wired.com/news/privacy/0,66983-1.html?tw=wn_story_page_next1.

[123] Bob Sullivan, *Database Giant Gives Access to Fake Firms*, MSNBC, Feb. 14, 2005, http://www.msnbc.msn.com/id/6969799/.

[124] SOLOVE, *supra* note 119, at 170.

[125] Sullivan, *supra* note 123.

[126] ChoicePoint Inc., Current Report (Form 8-K), at 2 (Mar. 4, 2005), available at http://www.choicepoint.com (follow the "About ChoicePoint" Menu; then follow "Investor Relations"; then follow "SEC Filings" and search by date).

[127] Rivlin, *supra* note 118.

[128] United States v. ChoicePoint, Inc., No. 1-06-CV-0198,,(N.D. Ga. 2006) (available at http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf).

January of 2006 and ChoicePoint agreed to pay $15 million dollars, the largest civil penalty in FTC history.[129] The settlement terms also required ChoicePoint to "establish, implement, and maintain a comprehensive information security program designed to protect the security, confidentiality, and integrity of the personal information it collects from or about consumers."[130]

Not all security breaches involve complex fraudulent schemes. The AOL disclosure also demonstrates how employee error can expose private information. The readme file that AOL included with the search queries states: "the goal of this collection is to provide real query log data that is based on real users. It could be used for personalization, query reformulation or other types of search research."[131] It also asks users to cite a specific journal when using the data for research.[132] These statements suggest that the original intent was to release the search queries for small-scale academic research. In addition, AOL's apology blames employees for acting without approval.[133] If AOL's statements were truthful, employees made a careless mistake that resulted in serious consequences.[134]

Perhaps the most common type of security breach involves stolen or lost laptops.[135] Recent companies that lost laptops include Altria, Notre Dame University, KeyCorp, Electronic Registry Systems and many others.[136] Even the FTC has fallen victim to computer theft.[137] Privacy breaches often involve laptops because each employee carries a separate copy of private information. It only takes one of them to act carelessly for all the data to become compromised. In addition, computer hardware is an attractive target for thieves. Sometimes the thieves are unaware of the private information, which

[129] Press Release, Fed. Trade Comm'n, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006), available at http://www.ftc.gov/opa/2006/01/choicepoint.htm.

[130] *Id.*

[131] Sadetsky, *supra* note 3.

[132] *See id.*

[133] America Online's press release came the day after it released user search logs. *See* Press Release, America Online, *supra* note 9.

[134] AOL is not the only company that has made careless mistakes. Virginia Commonwealth University inadvertently emailed the "names, SSNs, local and permanent addresses and grade-point averages" of more than 500 students to other students. Privacy Rights Clearinghouse, *supra* note 14. Segal Group posted personal data including social security numbers of health providers on its website. *See id.* The Privacy Rights Clearinghouse contains several other examples. *Id.*

[135] *See* Robert Ellis Smith, *Laptop Hall of Shame*, FORBES.COM, Sept. 7, 2006, http://www.forbes.com/columnists/2006/09/06/laptops-hall-of-shame-cx_res_0907laptops.html.

[136] *See* Privacy Rights Clearinghouse, *supra* note 14.

[137] *See* Christopher Conkey, *FTC Reports Laptop is Stolen in the Latest U.S. Data Breach*, WALL ST. J., June 23, 2006, at B2.

minimizes the risk of privacy invasions.[138] However, thieves who initially target hardware could also discover and misuse private data. The mere possibility that one's private data is exposed could harm consumers' peace of mind.[139] In addition, some thieves may specifically target computer hardware or media that contains private information.[140]

IV. PART III: PRIVACY REGULATIONS

Congress has passed several laws in response to privacy breaches. One of the most important privacy laws is the Electronic Communications Privacy Act ("ECPA").[141] Title I of the ECPA modified the Wiretap Act of 1968.[142] The Wiretap Act originally concerned only wire and oral communication.[143] The ECPA expanded the Wiretap Act to include electronic communications as well.[144] It now punishes anyone who "intentionally intercepts . . . any wire, oral, or *electronic* communication."[145]

The word "intentionally" significantly narrows the scope of the ECPA's application.[146] For example, in *In re Pharmatrak, Inc. Privacy Litigation*, the defendant, Pharmatrak, contracted with pharmaceutical companies to collect information from their website users.[147] Although Pharmatrak only contracted to create general user profiles, it ended up collecting personally identifying information against the wishes of the pharmaceutical companies.[148] In a ECPA suit, the court found Pharmatrak guilty for intercepting electronic communications.[149] However, on remand, the district court found that Pharmartrak had obtained the information as a result of third party software errors.[150] It therefore granted summary judgment because the plaintiffs had not met the intent requirement.[151]

---

[138] *See id.*

[139] *Cf.* James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. COLO. L. REV. 1, 33 (2005) (discussing the difficulty of determining "the value of knowing that the details of one's life are not open to public view").

[140] *See* Bosworth, *supra* note 17.

[141] Electronic Communications Privacy Act, 100 Stat. 1848 (1986).

[142] *See id.;* Bartnicki v. Vopper, 532 U.S. 514, 524 (2001) (discussing the history of the Wiretap Act).

[143] *See Bartnicki*, 532 U.S. at 524.

[144] *See id.*

[145] 18 U.S.C. § 2511 (2002).

[146] William DeCoste, *Sender Beware: The Discoverability and Admissibility of E-Mail*, 2 VAND. J. ENT. L. & PRAC. 79, 88 (2000).

[147] *In re* Pharmatrak, Inc., 329 F. 3d 9, 12 (1st Cir. 2003).

[148] *See id.*

[149] *See id.* at *22*.

[150] *In re* Pharmatrak, Inc., 292 F. 3d 263, 268 (2003).

[151] *Id.* at 268.

Several courts have also narrowly construed the word "intercept".[152] Under this interpretation of the Wiretap Act, acquisition of the message has to be contemporaneous with transmission.[153] However, email messages are often stored for short amounts of time during transit from party to another.[154] It is when they are in temporary storage that they are most vulnerable to eavesdropping.[155] The Wiretap Act would afford little protection to these actions since they are not contemporaneous with transmission.[156] In *Konop v. Hawaiian Airlines, Inc.*, the court applied the same analysis to web pages.[157] Presumably this limitation would also apply to other transmissions. These constructions of the ECPA severely limit the scope of the Wiretap Act.

Title II of the ECPA created the Stored Communications Act ("SCA").[158] Among other things,[159] the SCA provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service."[160] The prototypical example of an electronic communication service is an ISP such as AOL.[161] It provides for a similar prohibition applying to "remote computing services",[162] defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[163] Conceivably, the plain text of this provision could apply to many of the examples discussed in Part I. For example, a website that stores a cookie on the user's computer or that requires registration seems to be providing a "storage or processing service." However, recent court decisions have held that only the ultimate provider of Internet services falls under the ECPA.[164] Under this logic, an airline company that

[152] *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002) (agreeing with the narrow definition of intercept propounded by Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994) and United States v. Smith, 155 F.3d 1051 (9th Cir. 1998)).

[153] *See Konop*, 302 F.3d at 878.

[154] *See* DeCoste, *supra* note 146, at 89.

[155] *Id.*

[156] *Id.*

[157] *See Konop*, 302 F.3d at 878.

[158] Electronic Communications Privacy Act, 100 Stat. 1848 (1986) (codified at 18 U.S.C. 2701 et seq.).

[159] *See* 18 U.S.C. §§ 2701-10.

[160] 18 U.S.C. § 2702(a)(1) (2002).

[161] *See* McVeigh v. Cohen, 983 F. Supp. 219 (D.C. 1998) (describing AOL as an "online service provider").

[162] 18 U.S.C. § 2711(2) (2006).

[163] *Id.*

[164] *See In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299 (D.N.Y. 2005) at 307-08; Garcia v. Haskett, 2006 U.S. Dist. LEXIS 46303 (D. Cal. 2006) at 12.

provides registration services is not bound by the ECPA.[165] This interpretation probably limits the scope of this section to ISPs and email providers.

The ECPA's limitations make it largely ineffective at preventing privacy breaches. Part of the problem resulted from modifying the Wiretap Act, which originally focused only on oral and wire communications.[166] By extending the Wiretap Act to cover electronic communications, Congress may have stretched the statutory language further than logical construction permits.[167] Furthermore, Congress passed the ECPA in 1986 when the Internet was still in nascent form.[168] Congress could not have predicted the Internet in its current manifestation. These factors combine to make the ECPA "a complex, often convoluted, area of the law,"[169] and ineffective at policing the privacy practices of Internet companies.

Another well-publicized privacy law is the Children's Online Privacy and Protection Act ("COPPA").[170] COPPA prohibits the collection of personal information from a child (defined by someone younger than 13) unless the website gets "verifiable" parental consent.[171] The act also requires website operators to inform parents what personal information they have obtained regarding their child upon request.[172] The FTC provides the main enforcement for COPPA.[173] Marcy Peek has criticized COPPA by noting how companies can exploit loopholes in the legislation by posting boilerplate privacy policies, having users check a box stating they are thirteen or older, or simply claiming that they do not collect information from children.[174] These methods are effective because the FTC has interpreted COPPA violations as requiring "actual knowledge" that the website is collecting information from a child.[175]

The ECPA and COPPA are typical of the United State's sectoral approach

---

[165] *See JetBlue*, 379 F. Supp. 2d at 307-08.

[166] *See Bartnicki*, 532 U.S. at 524.

[167] *Cf. Konop*, 302 F.3d at 878 (deciding on a narrow definition of "intercept" by differentiating ECPA's effect on wire communications with its effect on electronic communications).

[168] Computer History Museum, *A History of the Internet 1962-1992*, http://www.computerhistory.org/exhibits/internet_history (last visited Apr. 2, 2007).

[169] United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998); *see also* Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 462 (5th Cir. 1994) (noting that the Wiretap Act "is famous (if not infamous) for its lack of clarity"; Konop v. Hawaiian Airlines, Inc., 308 F.3d 868, 874 (9th Cir. 2002).

[170] Children's Online Privacy and Protection Act, 112 Stat. 2681-728 (1998) (codified at 15 U.S.C. § 6501 et seq.).

[171] 15 U.S.C. §§ 6501, 6502 (2006).

[172] 15 U.S.C. § 6502 (2006).

[173] 15 U.S.C.. § 6505(d) (2006).

[174] Marcy E. Peek, *Information Privacy and Corporate Power: Towards a Re-Imagination of Information Privacy Law*, 37 SETON HALL L. REV. 127, 153-54 (2006).

[175] *Id.* at 154.

to privacy law.[176] Under this framework, laws target a specific industry or type of data instead of private data in general.[177] Other examples of sector-specific privacy laws include the Health Insurance Portability and Accountability Act ("HIPPA"), the Gramm-Leach-Bliley Act ("GLBA"), and the Fair and Accurate Credit Transaction Act ("FCRA").[178] The current patchwork of laws fails to provide safeguards against data collectors that fall outside of the regulated industries.[179] For example, an online dating site might contain very personal information about its customers, but it probably remains outside of the scope of regulation.[180] As noted above, the laws often have limited impact even on the industries or types of information that they attempt to regulate.

One reason that vast areas of data collection remain unregulated is because Congress tends to enact privacy legislation only in response to significant privacy breaches. This reactive approach leads to narrowly tailored laws.[181] For example, during the contentious Robert Bork confirmation hearings, the Washington City Paper published a list of Bork's video rentals.[182] Many legislators took offense to this breach of privacy and introduced legislation to prohibit the release of private video rentals.[183] As a result, Congress passed the Video Privacy Protection Act ("VPPA").[184] VPPA prevents the disclosure of a customer's video rentals and provides for a private right of action where the law has been broken.[185] However, the legislation does little to regulate similar businesses such as bookstores or music retailers.[186]

Congress's focus on self-regulation may help explain its sectoral approach to privacy regulation. In the 1960s and 1970s, Congress considered

[176] *See* Solove, *supra* note 119, at 67.

[177] *See* Solove, *supra* note 119, at 67. Compare this approach to European Union privacy law which relies on comprehensive data regulation. *See* Gerhard Steinke, *Data Privacy Approaches from US and EU perspectives*, 19 TELEMATICS AND INFORMATICS 193, 195-96 (2002).

[178] *See Generally* Nehf, *supra* note 24, at 5-15.

[179] Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 152 (2006); *see also* Nehf, *supra* note 24, at 5.

[180] An online dating website is not an ISP or Email provider, does not deal with credit reports, is usually accessed by people over the age of 13, and does not deal with health records. As a result, many of the major privacy regulations such at ECPA, COPPA, FCRA, and HPPA would not affect it.

[181] Ludington, *supra* note 179, at 152.

[182] Michael Dolan, *The Bork Tapes*, WASHINGTON CITY PAPER, Sept. 25 - Oct. 1, 1987, available at http://www.theamericanporch.com/bork2.htm.

[183] Ludington, *supra* note 179, at 153.

[184] Solove, *supra* note 119, at 69.

[185] 18 U.S.C. § 2710 (2000).

[186] Ludington, *supra* note 179, at 153; *see also* Solove, *supra* note 119, at 69 (financial privacy regulations provide another example of narrowly focused solutions). *See* Ludington, *supra* note 179, at 156-58.

establishing a federal agency which would oversee privacy across industries.[187] However, Congress rejected this solution in favor of an approach where companies monitor their own behavior.[188] Several commentators view recent data breaches as proof that self-regulation will never work. [189] They often proscribe large-scale privacy regulations.[190] However, wholesale regulation of private information presents its own problems. First, it is difficult for legislation to address the different concerns posed by industries as diverse as health-care, financial records, and entertainment. For example, even though the COPPA only regulates children's private information, it cuts across industries. While it might be appropriate to require parental consent for a website advertising toys to children, it might put an undue burden on websites that sell products targeted at adults. Broader legislation may exacerbate the problem and impede the growth of e-commerce.[191] Second, many consumers may wish to share their personal data in exchange for information which is targeted towards their tastes. Broad legislation might prove inflexible and not accommodate consumers who value their privacy differently.[192] Finally, even if Congress were to decide to pass comprehensive legislation, commentators disagree as to which solution will best protect online privacy.[193] These considerations have led Congress to adopt a market-based approach to privacy.[194]

The market-based solution to privacy problems can only succeed if consumers have adequate knowledge about how companies will treat their private information. Privacy policies are the best sources of this information. In an ideal world, the consumer could shop for privacy policies that match their preferences. Some companies already promote their privacy policies as a

[187] Nehf, *supra* note 24, at n.144.

[188] *Id.* at 46-47.

[189] Marcey L. Grigsby, Book Note, 50 N.Y.L. SCH. L. REV. 1031, 1035 n.33 (2005) (reviewing Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age (2004)).

[190] *See generally.* Solove, *supra* note 120 (suggesting several cross-industry regulations); Ludington, *supra* note 179, at 146. (suggesting a new common law torts for victims of data breaches); Kathryn E. Picanso, *Note: Protecting Information Security Under a Uniform Data Breach Law*, 75 FORDHAM L. REV. 355, 388-91 (2006) (suggesting, among other things, a federal data breach notification law similar to that of California).

[191] *See* Goldman, *supra* note 43, at 378; Solveig Singleton, *Privacy and Human Rights: Comparing the United States to Europe*, CATO WHITE PAPERS AND MISCELLANEOUS REP., Dec. 1, 1999, http://www.cato.org/pubs/wtpapers/991201paper.html.

[192] Fred Cate, PRIVACY IN PERSPECTIVE 26 (2001).

[193] *See* Goldman, *supra* note 43, at 379 (arguing that plurality of proposed solutions contributes to the lack of legislation regarding privacy); sources cited *supra* note 190.

[194] *See* Goldman, *supra* note 43, at 379. For analysis about the political and structural obstacles to passing privacy legislation, *see* PRISCILLA M. REGAN, LEGISLATING PRIVACY : TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 174-211 (1995).

selling point.[195] Consumers may take into account several factors when choosing to interact with Internet companies including the strength of security measures, the number of previous privacy breaches, and policies on sharing the information with other companies. As a result companies may modify their privacy standards to attract goodwill. For example, Google recently announced that it will delete identifying information after storing it for 18 to 24 months.[196] Google also gained popularity among the Internet community for refusing to turn over search requests pursuant to the DOJ subpoena discussed above.[197] Almost all of the major websites have privacy policies and even less popular websites usually give some information about how they use private information.[198]

Market-based solutions also require dependable privacy policies. If companies can violate their policies without penalty, consumers will have little control over their private information. To address this issue, the FTC has interpreted "unfair and deceptive practices" under the FTC Act[199] to include violations of privacy policies.[200] This allows the FTC to enforce privacy policies by punishing companies that violate them.[201] After the ChoicePoint privacy breach, for example, count IV of the FTC complaint was a violation of ChoicePoint's privacy policies.[202] The FTC has brought suit against other companies that have violated their privacy policies as well.[203]

The market-oriented approach also rests on the premise that companies and individuals have sufficient economic incentives to keep information private.[204] To a certain extent, this "patched-up" market-based approach has been successful. Companies have developed safeguards to prevent privacy breaches and the negative publicity that comes with them. Generally, Internet consumers are aware that some of their privacy is at risk.[205] They can take steps to choose companies that are more careful with their information.[206]

---

[195] *See* Cate, *supra* note 192, at 24-25.

[196] *See* Verne Kopytoff, *Google to tighten its rules to shield requests; Data won't hold identifying links after 18-24 months,* SAN FRANCISCO CHRONICLE, Mar. 15, 2007 at C3.

[197] *See* Editorial, *Google's Tangled Web*, HARTFORD COURANT, Jan. 30, 2006, at A6.

[198] *See* FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC Marketplace 10-11 (2000).

[199] Federal Trade Commission Act, 15 U.S.C. § 45 (2000).

[200] *See* Solove, *supra* note 119, at 72.

[201] *See id.*

[202] Complaint at 9-11, United States v. ChoicePoint, Inc., No. 06-CV-0198 (N.D. Ga. Jan 30, 2006).

[203] Solove, *supra* note 119, at 72.

[204] Nehf, *supra* note 139, at 18-20.

[205] Nehf, *supra* note 139, at 19.

[206] Goldman, *supra* note 43, at 379 (describing the argument that "privacy-conscious consumers will become more attracted to websites with better protection" and vote with their "eyeballs.").

However, as recent privacy breaches demonstrate, these small successes have not been able to prevent the growing number of privacy breaches.

V. PART IV: STATUS QUO PRIVACY POLICIES

As mentioned above, successful market solutions to privacy issues depend on consumers' ability to understand and analyze privacy policies.[207] If consumers cannot compare one privacy policy to another, they will be unable to effectuate their preferences. Unfortunately, privacy policies are usually long, complex, and difficult to understand.[208] They often include undefined terms[209] or legal concepts that are unfamiliar to most consumers.[210] Conspicuously missing from most privacy policies is what the companies *can* do with consumer information.[211] As Daniel Solove puts it, "[p]rivacy policies tend to be self-indulgent, making vague promises such as the fact that company will be careful with data; that it will respect privacy; that privacy is its number one concern."[212] The problems with current privacy policies increase the cost to the consumer in analyzing and selecting between online companies. Consumers who value their privacy highly will have to compare privacy policies from several competing websites. Considering the length and ambiguity of the policies, careful consumers would have to spend a significant amount of time combing through policies just to engage in routine online activities. Even if consumers take every precaution there no guarantee that they will not misinterpret essential language.

Again, AOL provides a good example of how difficult it is to interpret privacy policies. AOL's privacy policy states that "[y]our AOL Network information will not be shared with third parties unless it is necessary to fulfill a transaction you have requested, in other circumstances in which you have consented to the sharing of your AOL Network information, or except as described in this Privacy Policy."[213] At first glance this privacy policy seems

---

[207] Knowledge@Wharton, *Up for Sale: How Best to Protect Privacy on the Internet* (Mar. 19, 2001), http://knowledge.wharton.upenn.edu (search for article title) (quoting Mark Schwartz) ("These decisions presume a very high level of understanding on the part of consumers as to how the information they provide is being used or collected. But consumers don't have that understanding.").

[208] *See* Fishman, *supra* note 28, at 1543-47 (comparing the privacy policies of different retail "card memberships"); John Schwartz, *Privacy Policy Notices Are Called Too Common and Too Confusing* , N. Y. TIMES, May 7, 2001, at A1 (discussing financial privacy policy notices required by the GLBA).

[209] *See* Fishman, *supra* note 28, at 1544 (discussing the inability to discover the definition of "affiliated companies").

[210] *See* Will Rodger, *Privacy Isn't Public Knowledge Online Policies Spread Confusion With Legal Jargon*, USA TODAY, May 1, 2000, at 3D.

[211] *See* Peek, *supra* note 174, at 134-35.

[212] Solove, *supra* note 119, at 83.

[213] AOL, Privacy Policy - About AOL, http://about.aol.com/aolnetwork/aol_pp (last

secure. Still, it is unclear whether AOL's data breach, discussed above, fits under one of the policy's many exceptions. For example, the policy permits disclosure of information "to conduct research about your use of the AOL Network."[214] A consumer might easily miss this exception to AOL's policy. Furthermore, the policy does not specify whether any research would be conducted internally by AOL, by educational parties, or by third party data vendors. This uncertainty might frustrate consumers trying to select between ISPs and eliminate the incentives for companies to match privacy policies to consumer desires.

Most consumers decide not to read privacy policies before visiting a new website.[215] Instead they might use the company's trademark and reputation as a proxy for how carefully it protects private information.[216] Unfortunately, this technique is a poor predictor of how the company actually treats private information. Even if a company has suffered negative press due to a recent data breach, consumers may not be aware of the incident.[217] In fact, companies who have recently suffered a data breach often try to improve their reputation by dedicating large portions of their website to privacy information.[218] This increased focus on security may mislead consumers who would prefer not to deal with companies who have erred in the past. Until consumers can adequately evaluate competing privacy policies, the market-based solution will fail to protect privacy interests.

Even if consumers were able to completely understand privacy policies they still face an absence of meaningful choice. This problem is linked to the problem of complex and difficult to understand privacy policies. If consumers cannot interpret privacy policies, companies have little incentive to improve them. Some commentators also attribute the lack of choice to "industry leaders who have a firm stranglehold on the industry and who have adopted virtually the same pro-business privacy policies."[219] The market-based solution to privacy depends on a variety of different privacy policies. A solution to the current privacy system will have to promote meaningful options for consumers.

Finally, weak enforcement mechanisms fail to deter companies from violating their privacy policies. As mentioned above, the FTC can police privacy policies by bringing suit for "unfair and deceptive" business practices. However, the FTC seems powerless to stop the growing number of data breaches. Peek suggests three explanations for FTC's inability to deter privacy

visited Nov. 17, 2006).

[214] *Id.*

[215] *See* Solove, *supra* note 119, at 82.

[216] *See* Nehf, *supra* note 139, at 23.

[217] *See* Picanso, *supra* note 190, at 360-61.

[218] For example, ChoicePoint now has an entire website dedicated to its privacy policy. Privacy at ChoicePoint, http://www.privacyatchoicepoint.com/ (last visited Mar. 31, 2007).

[219] Peek, *supra* note 174, at 164.

violations.[220] First, the FTC rarely chooses to enforce privacy policy violations.[221] Second, when the FTC does choose to enforce violations, it focuses on well-known companies that "bring in headlines . . . for the government."[222] Many small and medium sized companies are not held accountable. Finally, the suits tend to settle for relatively small amounts of money.[223] Sometimes the FTC even settles the suit solely in exchange for a promise to correct any unfair practices.[224] Adding to the problems of enforcement, many companies retain the right to change their privacy policies at will.[225] Even if companies inform their customers of changes to their privacy policies, customers may feel trapped because of the hassle and complications of switching companies. As a result, consumers that manage to decipher and select an adequate privacy policy have no guarantee that the company will honor its promise. Without regular and effective penalties companies will continue to violate privacy policies when it is in their best financial interest.

VI. PART V: SOLUTION: STANDARDIZED PRIVACY POLICIES

One proposed solution that has met with limited success is the advent of privacy seals. Typically an independent company or a coalition of businesses establishes minimum privacy standards for participating websites. Websites that meet these guidelines can post a privacy seal which may attract privacy-conscious consumers. Privacy seal certification marks attempt to reduce the search costs of finding secure and reliable data handlers. TRUSTe is one of the most prevalent privacy seals.[226] Companies can apply online at the TRUSTe website by submitting their privacy policies. If the company meets TRUSTe guidelines and its website passes a website audit and review, it can display the TRUSTe seal on its website.[227] In theory, consumers should be able to use TRUSTe and other privacy seals to avoid the time consuming and frustrating task of analyzing and selecting privacy policies. Instead, they could limit their dealings to companies certified by privacy seal organizations. Unfortunately, as currently implemented, privacy seals cannot solve the

[220] *See* Peek, *supra* note 174, at 156-57.

[221] *See* Peek, *supra* note 174, at 156.

[222] Peek, *supra* note 174, at 156-57.

[223] *See* Peek, *supra* note 174, at 157.

[224] *See* Solove, *supra* note 119, at 72.

[225] *See* Solove, *supra* note 119, at 83 ("Yahoo!'s privacy policy indicates that it 'may change from time to time, so please check back periodically'").

[226] *See* TRUSTe, http://www.truste.org (last visited Jan. 28, 2007); *See* Federal Trade Commission, *Self Regulation and Privacy Online: A Report to Congress* (July 1999) at n. 9-10, available at http://www.ftc.gov/os/2000/07/onlineprofiling.pdf. For another privacy seal organization, *see* BBB, http://www.bbbonline.org (last visited Jan. 28. 2007).

[227] *See* TRUSTe, Begin Building Trust Now, http://www.truste.org/businesses/how_to_sign_up.php (last visited Jan. 28, 2007).

problems with privacy policies.

The most serious obstacle to web seal success is that few companies value seals enough to voluntarily adopt them. As of September 2005, TRUSTe had only certified 2,598 websites.[228] Among the ten most popular websites,[229] the majority lacked TRUSTe seals.[230] In addition, several members of TRUSTe fail to display their seals prominently.[231] As a result, it is almost impossible for consumers to limit their interactions to websites that display a privacy seal.

Another problem with privacy seals is that they limit privacy choices to a take-it-or-leave-it proposition. Consumers who prefer a higher privacy standard than the one propagated by the seal organization must revert to interpreting privacy policies.[232] The same problem applies to someone who is willing to settle for less protection but who still wants some minimum level of protection.

Finally, privacy seal organizations suffer from the same enforcement issues as the FTC. Several companies who received the TRUSTe seal violated their privacy policy anyways.[233] For example, Toysmart was a TRUSTe member when it attempted to sell its customer list.[234] Privacy seal organizations have little recourse besides revoking the seal and reporting the violation to the FTC. Additionally, to detect the problem, privacy seal organizations encounter the same problems as consumers—they have to interpret vague and complex privacy policies.

Despite these problems, privacy seals contain the framework for a solution. Congress can increase the benefits of privacy seals without superseding market-based solutions. Specifically, I suggest that Congress should delegate the power to award and enforce privacy seals to the FTC. Companies that wish to receive a privacy seal would have to select among standardized privacy policies instead of writing their own. Ideally, the FTC would accept input from data brokers, advocacy groups, current privacy seal organizations, and individual consumers. It would then come up with a "menu" of policies that companies could choose from. The policies should include such factors as: (1)

---

[228] *See* TRUSTe, Fact Sheet, http://www.truste.org/about/fact_sheet.php (last visited Jan. 28, 2007).

[229] *See supra* note 30.

[230] TRUSTe, Member List, http://www.truste.org/about/member_list.php (last visited Jan. 28, 2007) (google.com, baidu.com, youtube.com, myspace.com, orkut.com, qq.com, and sina.com.cn all lack TRUSTe seals).

[231] AOL is a member of TRUSTe. *Id.*; However there is no reference to TRUSTe on AOL's privacy policy page. *See* Privacy Policy, *supra* note 171.

[232] Nehf, *supra* note 24, at 64-65 ("for example, TRUSTe certifies sites that promise not to share information 'used to identify, contact, or locate a person.' Yet reports show that most Internet users do not want Web sites tracking their movements even if the site does not associate the data with a particular user's identity.") (footnotes omitted).

[233] *See* Sandoval, *Failed dot-coms*, *supra* note 72.

[234] *See id.* Other violations include boo.com, *id.*, and RealNetworks, *See* Givens, *supra* note 59, at 352.

whether the company collects information without explicit consent, (2) whether the company retains the right to sell or exchange third part information, (3) whether the company agrees to notify all customer in case of a data breach,[235] (4) whether the company deletes unnecessary data after a certain period of time,[236] and (5) the company's subpoena policy.

Depending of what level privacy policy the company selects, it would display a different, easy to recognize logo. The FTC would mandate that the company prominently display the logo on its privacy page. Some companies would undoubtedly want to display the logo on their main page to advertise their security. This system would be analogous to the Motion Picture Association of American's movie rating system or the National Highway Traffic Safety Administration's crash test ratings.

This solution would solve many of the problems with current privacy policies. First, it would promote greater transparency. Consumers who want control over how companies handle their private data need only learn a limited number of privacy policies. Although the legal language of each separate privacy level might be difficult to understand, the FTC or other consumer protection websites could translate each policy into "plain English."[237] Instead of relying on imperfect proxies for privacy standards, such as company reputation or third party seals, consumers could rely on the FTC privacy level.

A standardized privacy policies regime would also promote more choices for consumers. Some of the privacy levels would be above current industry standards. This would help create competition among rival websites.[238] Some websites might choose to make money by adopting a lower privacy level and selling visitors' information. Another might try to attract more visitors by displaying the logo for a higher privacy level. As a result, consumers will be better able to satisfy their privacy preferences. Unlike most proposed legislation, this solution also avoids patronizing consumers and companies.[239] Instead of mandating a certain level of privacy, standardizing privacy policies will encourage market solutions that reach an optimal solution.

Of course, legislation could not hope to mandate seals for every website that collects private information. Indeed this would be undesirable as some website may want to forgo having a restrictive privacy policy.[240] Still, most companies

[235] California has recently pass a law that would require all companies to inform their customers after a data breach. *See* CAL. CIV. CODE 1798.82(a) (2005).

[236] As mentioned *supra*, Google has begun a policy of deleting information after 18-24 months. Kopytoff, *supra* note 196.

[237] Creative Commons employs a similar concept for copyright protection. *See* Creative Common Licencses, http://creativecommons.org/about/licenses/meet-the-licenses (last visited Apr. 3, 2007).

[238] *Cf.* Cate, *supra* note 195, at 24-25 (discussing how increased interest in privacy issues will cause consumers to demand better privacy safeguards).

[239] *See* Cate, *supra* note 195, at 26.

[240] For example, this may be true of websites that give consumers rewards in exchange

would have strong incentives to adopt privacy seals. As the public becomes more educated with the privacy level system, it will come to expect websites to display a seal. They will assume that websites that choose not to adopt a seal are risky and should be avoided. Congress or the FTC could expedite the process by requiring that industry leaders (defined by revenue, website hits, or some other metric) obtain a privacy seal or disclose that they have chosen not to. This might work especially well for ISPs since they deal with a high volume of private information but are concentrated enough to be regulated effectively.[241]

Standardization will help prevent each of the three categories of privacy breaches discussed in Part II. First, it will deter companies from intentionally violating their privacy policies. Since the FTC will be very familiar with the limited number of privacy policies, it will be easier to detect violations. Companies will also have less leeway to use their vague language to escape responsibility. Courts can develop precedent as what constitutes a breach of particular policies, further increasing predictability. Additionally, the FTC could require that companies who violate their policy be placed on probation. Probation might be represented by "negative seal" that would warn consumers of a recent data breach. These factors would serve as a powerful deterrent against intentionally violating privacy policies.

Standardized privacy policies will provide a framework for analyzing subpoenas as well. Privacy standards may contain language that will guide companies in deciding whether to produce private information. When companies do file a motion to squash, courts will be in a better position to evaluate the interests of internet users. For example, a high privacy level might weigh in favor of squashing the subpoena. A judge might also be better able to fashion an equitable solution if she fully understands and evaluates a standard privacy policy.

Finally, standardization will reduce the prevalence of security breaches. The deterrence elements mentioned above will create strong incentives to train employees above how to best handle data. Companies will also have a clearer understanding of their legal responsibilities based on a common understanding of their privacy standards. These factors might have prevented the ChoicePoint privacy breach because employers would have been less susceptible to social engineering. Standardizing privacy policies is therefore a powerful solution to most common data breaches.

for information. *See e.g.* sources cited *supra* note 53.

[241] *See* Catherine Crump, Note*, Data Retention: Privacy, Anonymity, and Accountability Online*, 56 STAN. L. REV. 191, 196 n.21 (2003) ("The ISP industry is quite concentrated, certainly to the point where government will be able to identify ISPs and hold them to certain regulatory requirements.").

VII. CONCLUSION

The legislation I propose is only a partial solution. Congress may need to continue adopting legislation for specific industries that warrant increased protections. In addition, the FTC may need additional powers and funding to take on the responsibility of supervising compliance with privacy levels. Still, standardized privacy policies would go a long way toward shifting the emphasis toward great transparency and accountability. As Marcy Peek notes,

> When both laypersons and legal scholars dismiss a social problem as trivial or, at the most, important but less deserving of attention than "real" social justice issues, that problem becomes relegated to the backwaters of social and legal thought. In turn, the social problem is virtually ignored by policymakers and the government. Yet consumer attitudes are shaped and guided not only by the government and the mass media, but also by private actors such as corporations via shared governance of information privacy law.[242]

Standardizing privacy policies will involve coordination between the government, consumers, and corporations. By making privacy policies more accessible, it will encourage further focus on privacy issues. Only then can market forces address the needs of both data handles and privacy conscious consumers.

[242] Peek, *supra* note 174, at 165.