The Privacy Merchants: What is to be done?

Amitai Etzioni[1]

Rights have been long understood, first and foremost, as protection of the private from the public, the individual from the state. True, we also recognize positive rights (such as socioeconomic rights) and the government's duty to protect citizens from violations of rights by other actors besides the state. However, when violations of privacy are discussed, the first violator that typically comes to mind is "Big Brother"—that is, the state.[2]

This Article focuses on the growing threat to privacy from private actors, specifically profit-making corporations. It briefly outlines a range of options aimed at protecting individual privacy against encroachment by private actors—and evaluate them within the prevailing normative, legal, and political context in the United States.

I. Corporate Surveillance, Tracking, Data Mining, and Profiling

Most informed citizens probably know by now that corporations collect information about them, but they may well be unaware of the extent and scope of the invasions of privacy that are now widespread. Many may be aware of tracking tools referred to as "cookies." Cookies are installed on one's computer by visited websites. They are used to identify the person and to remember his or her preferences. Some people learned to protect themselves from such tracking by employing software that allows one to clear cookies from one's computer. However, corporations have recently begun to install "supercookies" that are very difficult to detect, and if removed, secretly reinstall themselves.[3] As one report concluded: "This means that privacy-sensitive consumers who 'toss' their HTTP cookies to prevent tracking or remain anonymous are still being uniquely identified online by advertising companies."[4]

Major cell phone and mobile technology companies offer services that allow lovers, ex-spouses, lawyers, or anyone else to find out where a person is—and track their movements—by using the GPS capabilities of their cell phone.[5] A German politician who inquired about location storage information discovered that over a six-month period, his longitude and latitude had been recorded over 35,000 times.[6]

---

[1] I am indebted to Nathan Pippenger for research assistance on this paper and to Orin Kerr and Alex Platt for comments on a previous draft. I also greatly benefited from discussions with Gina Stevens.

[2] *See, e.g.*, SHANE HARRIS, THE WATCHERS: THE RISE OF AMERICA'S SURVEILLANCE STATE (2010).

[3] Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J. July 30, 2010, http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

[4] *See id.*

[5] Justin Scheck, *Stalkers Exploit Cell Phone GPS*, WALL ST. J., Aug. 3, 2010, http://online.wsj.com/article/SB10001424052748703467304575383522318244234.html.

[6] Noam Cohen, *It's Tracking Your Every Move, And You May Not Even Know,* N.Y. TIMES, Mar. 26, 2011, at A1.

There are two kinds of corporations that keep track of what Internet users buy, read, visit, drink, and who they call, email, date, and much else. Some merely track users' activity on their site as part of their regular business; recording purchases and viewed products helps them increase sales. This is true for nearly every major online retailer. Other corporations make shadowing Internet users—and keeping very detailed dossiers on them—their main line of business. One can call these the Privacy Merchants. They sell information to whoever pays the required price. In 2005, one such company—Choicepoint—had records on over 220 million people.[7] Professor Christopher Slobogin notes that the amount of information culled by corporate data miners

> can provide the inquirer with a wide array of data about any of us, including basic demographic information, income, net worth, real [sic] property holdings, social security number, current and previous addresses, phone numbers and fax numbers, names of neighbors, driver records, license plate and VIN numbers, bankruptcy and debtor filings, employment, business and criminal records, bank account balances and activity, stock purchases, and credit card activity."[8]

(In 2009, a law professor at Fordham University gained minor notoriety when he assigned his class to create a dossier on Justice Antonin Scalia using only the information they could find online—resulting in a 15-page file "that included the justice's home address and home phone number, his wife's personal e-mail address and the TV shows and food he prefers."[9]) Some Privacy Merchants even keep dossiers on any crimes a person has committed, divorces, political leanings, as well as interests in topics including religion, the Bible, gambling, and adult entertainment.[10]

Although several data-mining companies allow individuals to opt out of their databases, each separate company must be contacted individually, and even then information may still linger in some search results or web sites: Google, for example, generally does not remove search results if the information contained is truthful and not illegal.[11]

Privacy Merchants are limited by laws Congress (and states) have enacted that carve out subsets of data that they cannot freely trade in, especially medical and financial records. So far though, very little attention has been paid to the fact that information is fungible. Through a process that might be called "privacy violating triangulation," (PVT) one can readily derive much about a person's medical, financial, or other protected private side by using "innocent facts" not privileged by law. A piece of seemingly benign information—for instance, the number of days a person failed to show up for work, or if the person made special purchases, such as a wig--suggests volumes about one's medical condition. By

---

[7] *They're Watching You*, BUS. WK., JAN. 24, 2005. http://www.businessweek.com/magazine/content/05_04/b3917056_mz005.htm.

[8] Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 320 (2008).

[9] Noam Cohen, *Law Students Teach Scalia About Privacy and the Web*, N.Y. TIMES, May 18, 2009, at B3.

[10] Emily Steel, *A Web Pioneer Profiles Users By Name*, WALL ST. J, Oct. 25, 2010 http://online.wsj.com/article/SB10001424052702304410504575560243259416072.html.

[11] Riva Richmond, *How to Fix (Or Kill) Web Data About You*, N.Y. TIMES, Apr. 14, 2011, at B6.

building a portfolio of many such apparently innocuous facts, one could infer a great deal, effectively violating the realm of privacy surrounding individuals' most sensitive information. Thus, a study of Facebook shows "how the on-line social network data could be used to predict some individual private trait that a user is not willing to disclose (e.g. political or religious affiliation)."[12] More about this later.

Some individuals may think that they can protect themselves from tracking and dossiers by using pseudonyms and multiple "mailboxes." However, some companies have developed software to match pseudonyms used on message boards and blogs with real names and personal email addresses. [13] The subjects of this tracking—who are unaware that their anonymity has been stripped—include people who use online pseudonyms to discuss sensitive topics like mental illness.[14] As Eli Pariser reports, "Search for a word like 'depression' on Dictionary.com, and the site installs up to 223 tracking cookies and beacons on your computer so that other websites can target you with antidepressants."[15] One notes that the privacy of medical records is protected by law, but not "visits" to medical web sites or chat groups.

Many companies claim that they do not collect names—or that they disassociate names from dossiers. However, some companies keep a database of names on file. One such company, RapLeaf, states that it does not share its subjects' names with advertisers; but an investigation found that it does link those names to "extraordinarily intimate databases [...] by tapping voter-registration files, shopping histories, social-networking activities and real estate records."[16] And although the company indeed refrains from specifically sharing *names* with its clients, it did share personally identifiable information with them, such as unique Facebook account numbers that can be traced back to the account holder's name.[17]

Privacy advocates have sharply objected to the government's use of deep packet inspection (DPI)—a powerful tool used to analyze the contents of communications transmitted over the Internet—in large part because it is much more intrusive than merely tracking who is communicating with whom. (The difference is akin to reading letters versus examining the outside of an envelope to see who sent the letter and to whom it is addressed.) Now private companies are offering to perform DPI for Internet Service Providers to facilitate targeted advertising.[18]

---

[12] Jack Lindamood, et al., *Inferring Private Information Using Social Network Data*, (Paper presented at the 18th International World Wide Web Conference, Madrid, April 20-24 2009) http://www.utdallas.edu/~muratk/publications/www09pp242-lindamood.pdf.

[13] Julia Angwin & Steve Stecklow, *Scrapers' Dig Deep for Data on Web*, WALL ST. J, Oct. 12, 2010, http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html.

[14] *See id.*

[15] Eli Pariser, *What the Internet knows about you*, CNN, May 22, 2011, http://articles.cnn.com/2011-05-22/opinion/pariser.filter.bubble.

[16] *See*, Steel *supra* note 10.

[17] *See id.*

[18] Steve Stecklow & Paul Sonn, *Shunned Profiling Technology on the Verge of Comeback*, WALL ST. J, Nov. 24, 2010, http://online.wsj.com/article/SB10001424052748704243904575630751094784516.html.

In 2010, Facebook became the most-visited website in the United States,[19] nearing 700 million users in June 2011.[20] Facebook users put great amounts of personal information on their individual profiles, including their religious and political views, educational and professional background, interests, as well as photos and videos of themselves. Most importantly, unlike most other websites where individuals employ usernames or pseudonyms, Facebook is designed for people to use their real names. This makes it vastly more valuable to data miners who seek to gather personally identifiable information in order to assemble dossiers on the individuals. Furthermore, each individual's profile is linked to the profiles of their "friends," who may have different privacy settings allowing for broader access to shared data, such as photographs or group membership, than the individual chooses to exhibit on his or her own profile.

Facebook provides customizable privacy tools and some privacy protection, but it has faced consistent criticism that those protections are unreliable and difficult to manipulate.[21] As Facebook has introduced third-party applications (such as games) to its site, it has faced mounting difficulties in keeping its end of the bargain.

In a July 2010 letter to Representative John Conyers of the U.S. House Judiciary Committee, a Facebook official stated, "The question posed in your letter asks whether Facebook shares users' personal information with third parties without the knowledge of users. The answer is simple and straightforward: we do not. We have designed our system and policies so that user information is never shared without our users' knowledge."[22] It was a few months later, in October 2010, that the *Wall Street Journal* broke the story of extensive user privacy breaches by Facebook.[23] It discovered that popular Facebook applications were "providing access to people's names and, in some cases, their friends' names" to Internet tracking companies.[24] According to the *Journal*, the breach affected "tens of millions" of users—including those who were vigilant in setting their privacy protections—and was in violation of Facebook's stated policies.[25] In the same month, the *New York Times* reported on two studies that found that "in certain circumstances, advertisers—or snoops posing as advertisers [on Facebook]—may be able to learn sensitive profile information, like a person's sexual orientation or religion, even if the person is sharing that information only with a small circle of friends."[26]

In addition, the nearly-ubiquitous Facebook "Like" and Twitter "Tweet" buttons on websites "notify Facebook and Twitter that a person visited those sites even when users

---

[19] Jessica Guynn, *T. Rowe Price invests in Facebook*, L.A. TIMES, Apr. 15, 2011, http://latimesblogs.latimes.com/technology/2011/04/t-rowe-price-invests-in-facebook.html.
[20] Pascal Emmanuel Gobry, *Facebook: Now 700 Million Strong?* BUS. INSIDER, (May 31, 2011), http://www.businessinsider.com/facebook-700-million-2011-5.
[21] *Facebook faces criticism over privacy change*, BBC NEWS, Dec. 10, 2009, http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/8405334.stm.
[22] Juliana Gruenwald, *Facebook Defends Privacy Policies*, NAT. J., (July 27, 2010) http://techdailydose.nationaljournal.com/2010/07/facebook-defends-privacy-polic.php.
[23] Emily Steel & Geoffrey A. Fowler, *Facebook in Privacy Breach*, WALL ST. J, Oct. 18, 2010.
[24] *See id.*
[25] *See id.*
[26] Miguel Helft, *Marketers Can Glean Private Data on Facebook*, N.Y. TIMES, Oct. 23, 2010, at B1.

don't click on the buttons."[27] These widgets have been added to millions of web pages and they appear on more than one-third of the world's top 1,000 websites – and for sites with those widgets to track specific Facebook users.[28] The tracking (which is used for targeted advertising) continues until the user specifically logs out of their account, even if the user turns off their computer.[29]

One may argue that the private sector merely uses this information for commercial purposes, while the government may use it to jail people, suppress free speech, and otherwise violate their rights. However, one must note that the *violation of privacy by private agents has some similar effects to violations committed by government agents, effects that lead to discrimination and "chilling" of expression and dissent*. Thus, when gay people who seek to keep their sexual orientation private are "outed" by the media, or banks call in loans of those they find out have cancer, or employers refuse to hire people because they learn about their political or religious views, privacy is violated in a manner about as consequential as if the same violations had been carried out by a government agency.

II. Privacy Merchants in the Service of Big Brother

Even if one disregards the facts already cited, showing that corporate violations of privacy are far-reaching and chilling, one must note that the *information corporations amass is available to the government*. Laws may prevent the government from ordering a private company to conduct surveillance on innocent citizens not suspected of anything, or from generating dossiers that the government itself is banned from generating (in other words, when corporations act as government agents, they may be subject to the same or similar limitations the government must abide by). However, the government can and does use data already amassed by Privacy Merchants for their own sake. Nor do prevailing laws prevent private corporations from analyzing online activity with an eye towards the government's needs and shaping their privacy-violating data in ways to make them more attractive to government purchasers of their services. Indeed, because the government is such a large and reliable client, corporate data banks have a strong financial interest in anticipating its needs. The thesis that what is private does not stay private is far from hypothetical. As Professor Chris Hoofnagle notes, even though Congress limited the executive branch's amassing of personal information in the 1974 Privacy Act, "those protections have failed to meet Congress' intent because the private sector has done what the government has been prohibited from doing."[30]

According to Professor Daniel Solove, "for quite some time, the government has been increasingly contracting with businesses to acquire databases of personal information. Database firms are willing to supply the information and the government is willing to pay for it."[31] Solove points out that government can "find out details about people's race,

---

[27] Amir Efrati, '*Like' Button Follows Web Users*, WALL ST. J., May 19, 2011, at B1.
[28] *See id.*
[29] *See id.*
[30] Christopher Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L. L. & COM. REG. 595, 611 (2004).
[31] DANIEL SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 169 (2004).

income, opinions, political beliefs, health, lifestyle, and purchasing habits from the database companies that keep extensive personal information on millions of Americans."[32] Hoofnagle similarly warns that "private sector commercial data brokers have built massive data centers with personal information custom-tailored to law enforcement agents."[33] ChoicePoint, a major Privacy Merchant, has at least 35 contracts with government agencies, including the Department of Justice (through which it provides its databases to the FBI), as well as the DEA, the IRS, and the Bureau of Citizenship and Immigration Services.[34]

Another corporate data miner, Florida-based SeisInt, ran a massive database called MATRIX (Multi-State Anti-Terrorism Information Exchange), in a joint effort among several U.S. states to coordinate counterterrorism efforts.[35] The federal government paid $12 million to support the program, which SeisInt developed with extensive amounts of data, including individuals' "criminal histories, photographs, property ownership, SSNs, addresses, bankruptcies, family members, and credit information."[36] Even before the 9/11 attacks, the U.S. Marshals Service alone performed up to 40,000 searches every month using private data banks.[37] The exact number of contracts the government has made with corporate data miners is unknown, because many of the contracts are classified.[38] However, one 2006 government study found that at least fifty-two federal agencies had launched—or were planning to launch at the time of the study—at least 199 data-mining projects that rely on the services and technology of commercial data banks.[39]

Other government tracking and surveillance efforts have relied on private corporations. In 2006, it was disclosed that three major telecommunications providers, AT&T, Verizon, and BellSouth, had cooperated with the NSA to provide it with the phone call records of "tens of millions of Americans"—a program which, according to one source, was "the largest database ever assembled in the world."[40] The companies which agreed to work with the NSA provide phone service to over 200 million Americans, leading the program significantly closer to its ultimate goal: creating a database of every phone call made within the United States.[41] Other government projects relying on private sources include efforts by Homeland Security to secure air travel and the nation's borders

---

[32] *See id.* at 167.
[33] Hoofnagle, *supra* note 30, at 611.
[34] THE AMERICAN CIVIL LIBERTIES UNION, THE SURVEILLANCE-INDUSTRIAL COMPLEX: HOW THE AMERICAN GOVERNMENT IS CONSCRIPTING BUSINESSES AND INDIVIDUALS IN THE CONSTRUCTION OF A SURVEILLANCE SOCIETY 26 (Aug. 2004) *available at* http://www.aclu.org/FilesPDFs/surveillance_report.pdf.
[35] Solove, *supra* note 31,38 at 170.
[36] *See id.*
[37] Slobogin, *supra* note 8, at 320.
[38] Arshad Mohammed & Sara Kehaulani Goo, *Government Increasingly Turning to Data Mining*, WASH. POST, June 15, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/06/14/AR2006061402063.html.
[39] *See id.*
[40] Leslie Cauley, *NSA has massive database of Americans' phone calls*, USA TODAY, May 11, 2006, http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm.
[41] *See id.*

and a Pentagon program which collects data on teenagers to better target military recruitment efforts.[42]

Moreover, the trend is to extend this use, as evidenced by a 2011 FBI manual that enables agents to search for private citizens in commercial databases without prior authorization or even notification.[43] In 2011, Google revealed that the U.S. government made the most requests for Internet users' private data in 2010, with Google complying with 94% of these orders.[44]

One may well hold that some of the usages of private data banks by the government serve legitimate purposes, even if they are loaded with extensive dossiers on most adult Americans, rather than those for which there is some evidence or reason to suspect that they are violating the law. However, one must still note that from here on, whether such data banks are in the FBI headquarters or in some corporate office matters little. At most, they are just a click—and a payment—away.

The next segment of this article outlines differing approaches to the protection of privacy in the new world in which the traditional distinction between public and private realms, on which many normative and legal conceptions build, in particular those that concern privacy, are much less important and are becoming still less significant. The new amalgamated social world calls for cross-realm or holistic modes of deliberations and policymaking.

III. The Main Alternatives

The following deliberations draw on my sociological training and normative considerations and not on any legal preparation. I merely chart the "big picture" because – as will become clear shortly—most if not all the alternatives are facing major hurdles. It hence seems premature to spell out any of the alternative approaches before strategies and political forces are developed that will make it possible to overcome these hurdles. The alternatives are evaluated not on the basis of what would best protect privacy from Privacy Merchants—but which measures might be taken in the prevailing context in the United States.

A. Change the Norm: A World Without Privacy?

One major response to Privacy Merchants' expanding reach has been well encapsulated by the CEO of Sun Microsystems, Scott McNealy, who stated: "privacy is dead, get over it."[45] Facebook's founder, Mark Zuckerberg, argues that social norms undergirding privacy law are obsolete. That is, instead of finding new ways to protect

---

[42] Mohammed & Kehaulani Goo, *supra* note 38.
[43] Charlie Savage, *FBI Agents Get Leeway to Push Privacy Bounds*, N.Y. TIMES, June 13, 2011, http://www.nytimes.com/2011/06/13/us/13fbi.html.
[44] GOOGLE TRANSPARENCY REPORT, (June 2011) http://www.google.com/transparencyreport/governmentrequests.
[45] Polly Sprenger, *Sun On Privacy: 'Get Over It,'* WIRED, (January 26, 1999), http://www.wired.com/politics/law/news/1999/01/17538.

individuals from corporations, individuals should learn to accept changed—in effect, much lower—levels of privacy. He elaborated: "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people [...] That social norm is just something that has evolved over time."[46] Zuckerberg continued: "We view it as our role in the system to constantly be innovating and be updating what our system is to reflect what the current social norms are."[47] He thus implies that the Privacy Merchants are not undermining the norm, but merely accommodating their wares to already in-place changes in norms.

As I see it, it is true that the privacy norms are eroding due to other factors than the corporate drive to use private information for profit making, as one sees with people going on talk shows to reveal much about themselves, a form of exhibitionism. However, there can be little doubt that corporations, especially the new social media, led by Facebook, are aiding and abetting and seeking to legitimate the erosion of privacy.

The *Wall Street Journal* editorial page, which reflects that publication's philosophy, argues that the change in norms indicates that the introduction of new laws or regulations to better protect privacy is not called for. L. Gordon Crovitz pointed out that, as of March 2011, more than half of Americans over twelve have Facebook accounts.[48] He proceeded to ask: "If most Americans are happy to have Facebook accounts, knowingly trading personal information for other benefits, why is Washington so focused on new privacy laws? There is little evidence that people want new rules."[49]

Furthermore, Crovitz argues, consumers value the benefits of information gathering, including better-targeted ads, specific recommendations for customers, and huge troves of data for research (such as in Google Flu Trends, which tracks search terms about illnesses to assist epidemiologists). "People are increasingly at ease with sharing personal data in exchange for other benefits," he argues.[50]

Some public opinion polls, including recent ones, show that the American people care a great deal about their privacy. Others—that various segments of the public vary in the way they feel about this right. For example, according to a 2009 survey, 73 to 86% of Americans object to the tracking methods used to personalize their advertisements. Furthermore, the study found that 82% of young people—who are generally believed to be apathetic about privacy—had at some point refused to provide information to a company because it was too personal. 86% of Americans—84% among respondents aged 18 to 24—felt that their permission should be sought before pictures of them were posted online.[51]

---

[46] Bobbie Johnson, *Privacy no longer a social norm, says Facebook founder*, THE GUARDIAN, Jan. 11, 2010, http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy.
[47] Ian Paul, *Facebook CEO Challenges the Social Norm of Privacy*, PC WORLD, Jan. 11, 2010, http://www.pcworld.com/article/186584/facebook_ceo_challenges_the_social_norm_of_privacy.html.
[48] L. Gordon Crovitz, *The 0.00002% Privacy Solution*, WALL ST. J, Mar. 28, 2011, at A15.
[49] *See id.*
[50] *See id.*
[51] Joseph Turow et al, *Americans Reject Tailored Advertising and Three Activities that Enable It,* at http://repository.upenn.edu/asc_papers/137 (Sept. 29, 2009).

Other data reveal a more varied picture. In a 1995 survey, Alan Westin divided the public into three "camps" over privacy concerns. About 25% of respondents were "Privacy Fundamentalists," who value privacy especially highly; 55% were "Privacy Pragmatists," who adjust their expectations based on the relative value of information types and trust in specific companies; and 20% were "Privacy Unconcerned," who have no problem with giving out personal information.[52]

A 2002 study found that while 70% of consumers were concerned about their privacy, 82% were willing to give out personal information in exchange for the chance to win a hundred dollars in a sweepstakes.[53] The rise in popularity of location-tracking social networking sites such as Foursquare, Facebook Places, and Gowalla, which offer discounts to users who log visits to various businesses and restaurants, suggests that people are indeed willing to trade information once considered private (their locations and consumption habits) for certain benefits. According to one survey, the coupon reward systems on these sites were the main incentive for users to join.[54]

One must, though, take into account that it is very likely that those who have relatively little concern about privacy are unaware that their less sensitive information can be used for PVT, and—that privacy is a right, not subject to majority rule. Even if only a minority cherishes it, it is still a birthright of all Americans.

B. The Self-Regulation Option

The prevailing system in the United States—and the *de facto* prevailing system in the EU—relies to a significant extent on self-regulation and individual choice; that is, the assumption that consumers will choose the services and products of those corporations that protect privacy at the level the consumers seek. And that users can set their privacy controls to the level they prefer. And that, as a result, corporations that provide less privacy protection than the public seeks will lose business and be incentivized to enhance their privacy protection. (Additionally, some scholars have argued that marketing in this vein is protected as free speech under the First Amendment, an argument not addressed in this paper.)[55] These ideas are founded on the standard libertarian argument, as noted by Susanna Kim Ripken: "Respect for individual autonomy, responsibility, and decision-making is deeply entrenched in our culture and law. We believe that people can order their

---

[52] Alan Westin, *"Whatever Works": The American Public's Attitudes Toward Regulation and Self-Regulation on Consumer Privacy Issues*, *in* NATIONAL TELECOMMS. & INFO ADMIN., U.S. DEP'T OF COMMERCE, PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE ch. 1, § F (1997), *available at* http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1F.

[53] Bob Tedeschi, *Everybody Talks About Online Privacy, But Few Do Anything About It,* N.Y. TIMES, June 3, 2003, at C6.

[54] Matt Carmichael, *What Consumers Want From Brands Online,* AD AGE, (February 27, 2011), http://adage.com/article/digital/consumers-seek-brand-discounts-facebook-preferred-platform/149095.

[55] For further discussion, see A. Michael Froomkin, Symposium, *The Death of Privacy?* 52 STAN. L. REV (2000); and Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. LAW REV. 1051 (2000).

own economic affairs and, given sufficient information, can make their own personal assessments of the risks and benefits of transactions."[56]

None of these assumptions withstand sociological scrutiny. The thesis that consumers are rational actors who make decisions in their best interests, in line with their personal preferences and available information, has been disproven beyond reasonable doubt by the studies of behavioral economists.[57] For this very reason, transparency does not work. That is, the suggestion that if corporations simply declare what their privacy standards are, consumers could choose those that suit them, is erroneous if not misleading. The statements are written in legalese, in terms few can penetrate; the privacy settings provided are complex, cumbersome, and frequently revised—after the users have posted information on the site, which they cannot erase.

Furthermore, without regulation, there is no assurance that corporations will adhere to their privacy declarations, at least to their implied promise. [58] This does not refer necessarily to outright false statements, but to carefully crafted yet misleading commitments to privacy that end up entrapping the consumer. For instance, after public outcry over the iPhone's hidden location tracking, Apple released a statement denying that they tracked users' locations; rather, they maintained "a database of WiFi hot spots and cell phone towers around your current location." As Mark Rotenberg of the Electronic Privacy Information Center (EPIC) pointed out, this database is precisely how the company tracks locations, even if it is not tracking the device itself.[59] A study by DoubleVerify surveyed five billion advertisements and found that an icon explaining the privacy policy was clicked on only 0.002% of the time—and even then, after users reviewed the advertisers' information practices, only 1% opted out of the targeted advertising.[60] "That's an opt-out rate of just 0.00002%," Crovitz notes. "People seem to have adjusted to this new technology faster than regulators are willing to admit."[61] Crovitz argues that the fact few consumers read these statements shows they do not care; in actuality, data already cited strongly suggests that they do not use them because they find them impenetrable. [62] Another national survey found that 57% of adult Americans were under the false impression that if a website merely had a privacy policy, then it would not share their information with other

---

[56] Susanna Kim Ripken, *The dangers and drawbacks of the disclosure antidote: toward a more substantive approach to securities regulation*, 58 BAYLOR L. REV. 186, 195 (2006).

[57] For further discussion on this subject, see DAN ARIELY, PREDICTABLY IRRATIONAL: THE HIDDEN FORCES THAT SHAPE OUR DECISIONS 243 (2008).

[58] Chris Hoofnagle, *Can Privacy Self-Regulation Work for Consumers?,* TAP, (Jan. 26, 2011), at http://www.techpolicy.com/CanPrivacySelf-RegulationWork-Hoofnagle.aspx.

[59] Adam Satariano and Katie Hoffmann, *Apple Denies Tracking iPhone Locations, Will Update Software,* BLOOMBERG, (April 27, 2011), http://www.bloomberg.com/news/2011-04-27/apple-denies-tracking-iphone-locations-will-reduce-data-storage-capacity.html.

[60] Crovitz, *supra* note 57.

[61] *See id.*

[62] Federal Trade Commission, *FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers*, at http://www.ftc.gov/opa/2010/12/privacyreport.shtm (Dec. 1, 2010).

companies.[63] Moreover, *individuals cannot protect themselves from corporations* that employ covert tools such as Flash cookies, supercookies, and widgets.

Large corporations—which do business in all fifty states, as well as overseas—find it in their interest to promote regulation that would provide some modicum of privacy. This is the case because such corporations incur considerable costs when they have to adjust their way of doing business to different state laws, and deal differently in various segments of the market—some of which are more regulated than others, under the current patchwork of privacy laws.

Hence some large corporations once opposed to legislation now favor a federal omnibus privacy law that would simplify the patchwork of federal sector-specific laws and preempt state specific statutes. A Microsoft white paper from 2005 advised, "Federal privacy legislation should pre-empt state laws that impose requirements for the collection, use, disclosure, and storage of personal information."[64] Such a law would likely set standards and ceilings (for instance, caps on damages for privacy violations), which states could not exceed. State laws demanding higher privacy standards than a federally-mandated norm would be invalidated, or at least weakened significantly. Indeed, it seems they would accept only legislation that included preemption. Former CEO of eBay Meg Whitman explicitly testified before Congress, "Legislation without preemption would make the current situation possibly worse, not better, by creating additional uncertainty and compliance burdens."[65] The ideal legislation, for Microsoft and similar entities, would provide "baseline privacy protection" over which companies would be encouraged to "compete on the basis of more robust privacy practices"[66]—essentially regulate themselves. According to Microsoft Deputy General Counsel for Erich Anderson's testimony before Congress, a federal law should be crafted only as "an effective *complement* [emphasis his] to" self-regulation.[67]

State and sectoral laws have already addressed a number privacy issues (e.g. setting limits on tracking consumers for targeted advertising[68]) while Congress has been largely inactive in this area.[69] Hence, following this line would in effect reduce privacy standards in those states that lifted them and may prevent them from adding protections in the future.[70] And—the corporate proposal does involve some federal legislation rather than merely relying on self-regulation. Indeed, it seems impossible to restrain the Privacy Merchants without calling in Big Brother.

---

[63] Joseph Turow, *Americans and Online Privacy: The System is Broken,* Annenberg Public Policy Center Report, http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf. (June 2003).
[64] Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 921 (2009).
[65] *See id* at 929.
[66] *The Need for a Comprehensive Approach to Protecting Consumer Privacy: Hearing on the State of Online Conumer Privacy Before the Senate Comm. On Commerce, Science & Transportation,* 112th Cong. 6 (2011) (statement of Erich Anderson, Deputy General Counsel, Microsoft Corporation).
[67] *See id* at 8.
[68] H.B. 5765, General Assembly, February Session (Conn. 2008).
[69] Schwartz, *supra* note 64, at 946.
[70] Hoofnagle, *supra* note 58.

C. Consent for Secondary Use: Opt in Rather than Out?

A rather different approach holds that individuals who release information about themselves for a specific purpose or transaction, for example to purchase a book from Amazon, would be understood to still "own" this information, and that Amazon could use it for other purposes (or sell that information to other parties) only with the explicit consent of the consumer (rather than on the basis of a privacy statement on its web pages or presumed consent). The same idea is referred to in other words, namely that consumers would have to opt in to grant secondary and additional use of private information rather than opt out.[71] In American discourse, the term "owned" is used because information is treated as property and private information as private property. In Europe, the same idea is embraced; however, privacy is treated more as an individual right- as part of the personhood- which is violated when one's private sphere is violated.

In 1995, in an effort to establish minimum protections for Internet user privacy and establish a baseline consistency among the data protection laws of EU member states, the European Council issued what is commonly called the "Data Protection Directive." The Directive, which scholars have called "aggressive"[72] and "extraordinarily comprehensive,"[73] took effect in October 1998. Based on a legal tradition that "expressly recognizes the fundamental right to the protection of personal data,"[74] the Directive is credited with having established the most influential and prominent data protections in the world to date.[75] However, it has proven difficult to ensure compliance in those countries governed by the Directive. Although the law set out ambitious goals for the standardization of privacy protection in Europe, it has been hampered from the start by significant gaps in member states' compliance and enforcement. According to one observer, "although the EU Data Privacy Directive has been approved by the EU itself, it is not self-implementing. Before taking effect in individual nations, each of the fifteen EU member countries must pass its own implementing legislation. As of the effective date, only five had done so."[76]

The Directive requires that personal data be processed "only with the consent of the data subject,"[77] with limited exceptions carved out for national security, law

---

[71] For further discussion of consent-based approaches to privacy and information "ownership," see Julie E. Cohen, *Information Rights and Intellectual Freedom* in ETHICS AND THE INTERNET 11-32 (Anton Vedder, ed., Antwerp: Intersentia, 2001).
[72] Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERKELEY TECH. L.J. 461, 462 (2000).
[73] FRED H. CATE, PRIVACY IN THE INFORMATION AGE 36 (1997).
[74] Electronic Privacy Information Center, *Background: EU Data Protection Directive*, *available at* http://epic.org/privacy/intl/eu_data_protection_directive.html.
[75] Erica Newland, *CDT Comments on EU Data Protection Directive*, The Center for Democracy and Technology, (January 20, 2011), http://www.cdt.org/blogs/erica-newland/cdt-comments-eu-data-protection-directive; *see also* THE CENTER FOR DEMOCRACY AND TECHNOLOGY, COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY TO THE EUROPEAN COMMISSION IN THE MATTER OF CONSULTATION ON THE COMMISSION'S COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION IN THE EUROPEAN UNION, 7 (Jan. 15, 2011), http://cdt.org/files/pdfs/CDT_DPD_Comments.pdf.
[76] Fromholz, *supra* note 72, at 467-8.
[77] Cate, *supra* note 73, at 37.

enforcement, and some basic state functions such as taxation.[78] The intentionally broad language of the Directive includes—but is not limited to—such actions as collecting, storing, recording, adapting, retrieving, and erasing data;[79] and "data" itself is defined broadly enough to include not just text, but also photographs, video, and sound.[80] Its restrictions recognize that certain kinds of data are particularly sensitive and vulnerable to abuse; thus, it contains heightened restrictions on the processing of data which would reveal the subject's personal traits, such as race, ethnicity, religious beliefs, or health background. In most cases, collecting and passing on these kinds of information require the subject's *written* consent, or they cannot be processed.[81]

The law also requires a degree of transparency: data processors must disclose to subjects of processing the ways in which they intend to use the data.[82] Finally, in one of the Directive's most restrictive and controversial portions, the drafters attempted to address the "borderless" nature of the Internet and the likelihood that user data could be processed in or transmitted to countries not subject to the law's protections. To protect against this vulnerability, the Directive contains a provision requiring member states to prohibit the transfer of data to third countries that have not adopted an "adequate level of protection" for personal data.[83] However as we have seen, implementing these protections has proven difficult, and enforcement across Europe has, at best, proven inconsistent.

According to a 2011 report from the Center for Democracy and Technology, "although it is comprehensive in many ways, the [European] Data Protection Directive has significant weaknesses. Erratic enforcement and uneven implementation have left consumers and industry confused as to how the Directive's principles apply to emerging practices."[84]

In 2011, various EU authorities called for new stronger privacy protection measures, especially in response to Facebook; however, so far those have not been translated into new laws or regulations, not to mention enforcement.

Limiting the involuntary secondary use of private information is much more popular in Europe than in the U.S., as evidenced by the Directives enacted relatively early in the Internet's lifespan, while a comprehensive American approach has yet to be articulated. However, *the differences between the American and European approaches are much less pronounced than they may first seem*. This is the case (a) Because Europeans do allow involuntary secondary use for a variety of purposes, including national security, prevention of criminal activity, journalistic freedom of speech, and personal use (for instance, an

---

[78] *See id.*
[79] *See id* at 36.
[80] *See id.*
[81] *See id*
[82] *See id.*
[83] Fred H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431, 437 (1995).
[84] Newland, *supra* note 75.

address book);[85] (b) Because the U.S. has set limits on a variety of secondary use of what might be called "sensitive information;"[86] and (c) Because of what is called a "compliance gap"—that is, a gap between what is mandated by European laws and the extent to which the various governments enforce these laws.[87] The EU's privacy protections suffer from this gap.

The ban on involuntary secondary use burdens the consumers, who have limited capacity to evaluate various privacy statements and assurances that these are indeed heeded. They are unaware of the risks of PVT. And business lobbies tend to strenuously oppose this approach, which makes it very unlikely to be enacted in the United States or heeded in Europe. And differences in laws and enforcement levels among countries—across whose borders the same information readily flows—greatly limit the value of this way of better protecting privacy from private invasions.

D. Ban public use of private information?

Those who adhere to the traditional distinction between the public and private realm, and the precept that the main danger to privacy comes from Big Brother, may suggest that the way to proceed is to ban the government from using private data banks. The 1974 Privacy Act already states that the government may not *maintain* personal data records for citizens who are not the subjects of investigations;[88] it would be relatively simple to add that they also may not *use* existing records in the private sphere. Still, this would not be necessary if Privacy Merchants were limited to trading only in less sensitive information, and of little use if this were not the case. In the latter case, such a law would in effect assume that it is acceptable for data banks to be used for profit-making—but not for enhancing the common good, such as public health and security. (Security these days often brings to mind measures taken to prevent terrorist attacks. A considerable number of civil liberty advocates hold that these dangers have been exaggerated and hence rights are unduly curtailed. However, one should note that security also encompasses criminal justice systems, which have utilized data banks to curb criminals.[89])

E. Increased Public Regulation of Sensitive Information?

A limited approach to curbing Privacy Merchants entails expanding the American patchwork of sectoral laws that limit the violation of privacy in one specific area or another. As Gina Stevens catalogues, "Federal laws and regulations extend protection to consumer credit reports, electronic communications, federal agency records, education

---

[85] Article 13 of Council Directive 95/46/EC of the European Parliament and of the Council of 24 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. L 281/31.

[86] *See id.*

[87] For a discussion of this topic, see Ellen Mastenbroek, *EU Compliance: Still A 'Black Hole'?* 12 J. EUROPEAN PUB. POL'Y 1103-1120; *see also* Maria Mendrinou, *Non-compliance and the European Commission's Role in Integration*, 3 J. EUROPEAN PUB. POL'Y 1-22 (1996).

[88] 5 U.S.C. § 552a(e)(7)

[89] Amitai Etzioni, *DNA Tests and Databases in Criminal Justice: Individual Rights and the Common Good*, in DNA AND THE CRIMINAL JUSTICE SYSTEM 197-218 (David Lazer, ed. 2004).

records, bank records, cable subscriber information, video rental records, motor vehicle records, health information, telecommunications subscriber information, children's online information, and customer financial information."[90] One could add some more areas to this long but seemingly arbitrary list.

The patchwork of laws can be viewed as based on a rationale that treats differently three main areas—private information gleaned from public records (e.g. house ownership), relatively sensitive information (especially medical and financial), and information that is in effect deemed less sensitive (most consumer choices). The patchwork can be seen as largely based on the level of sensitivity of the information. Public records, therefore, are open for dissemination online because this information was not private in the first place; less sensitive information is considered in need of little protection because no or little harm is inflicted when it is used by third parties; and sensitive information is protected. And to the extent that one finds that some area is not well protected, the argument runs, one can add another "patch" of legislation to cover this area.

The patchwork approach has two serious defects, one often cited and one less often noted. It is widely recognized that the patchwork lags woefully behind technological developments in the private sector. Thus, legislation attempting to cover uncovered areas is "proposed" and "drafted" but not enacted. Thus, as of mid 2011, one suggested bill calls for a federal requirement of a "Do Not Track" option for online advertising. Another suggested bill would deal with the relatively new technology of geolocation and mobile privacy.[91] The Federal Trade Commission is reportedly working on a regulatory framework governing social networking sites, in the wake of high-profile FTC complaints against Google Buzz and Twitter. The FTC also plans to target smart phones, a market virtually untouched by regulation thus far.[92] However, these laws lag considerably behind the new technological developments employed by Privacy Merchants, and given the current anti-regulatory climate, are unlikely to be enacted.

Less often noted is the problem that the distinction between "sensitive" and "less sensitive" information is much less tight than it seems and is likely to further weaken in the near future. Even if sensitive information such as medical or financial records is better protected online, less sensitive—and therefore, less protected—information can reveal volumes of sensitive information through PVT. As Marcy Peek points out, "The Internet has allowed commercial decision-makers to manipulate technology in such a way as to identify persons according to a multitude of variables and categories."[93] Unique IP addresses are tracked by each page people visit and ad they click on to create a detailed portrait of the offline persona. Peek explains, "Through various means such as cookies, Web bugs, and personal data input such as zip codes, corporate marketers can obtain a

---

[90] Gina Stevens, *Privacy Protections for Personal Information Online*, CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, April 6, 2011.
[91] Katie Kindelan, *John McCain and John Kerry Propose "Online Privacy Bill of Rights,"* SOCIAL TIMES, (Mar. 10, 2011), http://socialtimes.com/john-mccain-and-john-kerry-propose-online-privacy-bill-of-rights_b41604.
[92] Tony Romm, *Will FTC get the funds it needs to police Internet?* POLITICO, June 3, 2011, http://www.politico.com/news/stories/0611/56134.html.
[93] Marcy Peek, *Passing Beyond Identity on the Internet: Espionage & Counterespionage in the Internet Age*, 28 VT. L. REV. 91, 94 (2003).

person's demographic and other information and "tag" an individual on the basis of such information." The individual is then categorized and ranked against other users. The result is "Weblining," an online version of the offline discriminatory practice of "redlining" individuals by denying or increasing the cost of services based on their demographic. After the Fair Housing Act of 1968 prohibited redlining, which used a mortgage applicant's neighborhood to discriminate along racial lines, banks used instead other markers of race as a basis for racial discriminations; for instance, which social club people joined or church they attended. That is, an item of information that is not sensitive was used to divine another item meant to be private. The easy access to this type of non-sensitive information online streamlines this practice.

As early as 2000, *Business Week* highlighted a PVT service offered by data broker company Acxiom called "InfoBase Ethnicity System," which matched names against housing, education, and incomes in order to identify the unpublicized ethnicity of an individual or group.[94] More recently, a computer consultant named Tom Owad wrote a simple piece of software allowing him to download public wish lists that Amazon.com customers post to catalog products they plan to buy. He downloaded over 250,000 wish lists in one day, used Yahoo People Search to identify addresses and phone numbers, and published a detailed map showing the locations of people interested in certain books or themes. Owad explained, "It used to be you had to get a warrant to monitor a person or group of people. Today, it is increasingly easy to monitor ideas. And then track them back to people."[95] And most people who put simple items of information about their preferences on their Facebook profiles are unlikely to know that it can be used to divine their personality traits with 90% accuracy, as if they had taken personality tests.[96]

All this suggests that laws that ban the use of sensitive information (without requiring any action by the millions of effected citizens), the way medical, financial, and select other records are now protected, could be reinforced by banning PVT of protected areas. That is, the wall that separates more sensitive and less sensitive information could be shored up. (Granted, the debate about what is sensitive and what is not would continue.) That is, the law would ban Privacy Merchants from using information on what one purchases (and other such 'less' sensitive information) to divine one's medical condition (and other such 'more' sensitive information).

Given the current pro-business and anti-regulatory climate in Congress, the Supreme Court, and, it seems, among the voters, enactment of such laws in the United States (and their enforcement in Europe, if enacted) may seem very unlikely. The prospect of such legislation improves if one notes that they would mainly curb those few corporations that make selling private information their main lines of business. Other corporations that merely keep profiles of their own customers' *consumeristic* preferences

---

[94] Marcia Stepanek, *Weblining*, BUS. WEEK (April 3, 2000), http://www.businessweek.com/2000/00_14/b3675027.htm

[95] Nicholas Carr, *The Dangers of Web Tracking,* WALL ST. J., Aug. 7, 2010, at W1.

[96] Jennifer Golbeck, Christina Robles & Karen Turner, *Predicting Personality with Social Media,* CHI EXTENDED ABSTRACTS 2011, 253-262.

would not be affected, although their ability to sell this information to other parties might be limited (to reduce the risk of PVT), and their advertising would be set back because corporations could not use sensitive information in their targeting. Nevertheless if such laws against PVT used to divine sensitive information could be enacted, they would serve as part of system that would shore up privacy to reasonable level in the future, in which I expected PVT otherwise to be much extended. It is better to ban this approach before it catches on widely then try to eradicate it once is it is widespread.

Conclusion

Corporations, especially those that make trading in private information their main line of business—the Privacy Merchants—are major violators of privacy, and their reach is rapidly expanding. Given that the information these corporations amass and process is also available to the government, it is no longer possible to protect privacy by only curbing the state. Suggesting that norms have changed and that people are now more willing to give up their privacy may be true, but only up to a point. The extent to which private aspects of one's medical and even financial conditions are revealed is unlikely to be widely accepted as a social good. And violation of the privacy of dissenters and, more generally, of one's political and social views (e.g. by tracking what people read) has chilling effects, whether or not the majority of the public understands the looming implications of unbounded profiling of most Americans. Self-regulation cannot come to the rescue because it assumes that individuals can sort out what corporations are doing behind the veil of their privacy statements, an unrealistic assumption. Banning the use of less sensitive information (in particular, about purchases) for divining more sensitive information (e.g., medical) — that is, outlawing Privacy Violating Triangulation—may serve, if combined with laws that add 'patches' to the current patchwork of legislation, to cover new technological developments (e.g. social media). If such twin progress is possible, there will be much less reason to prevent the government from drawing on the databanks maintained by Privacy Merchants, because they would be limited to less sensitive information, and PVT of innocent Americans would be banned. Without such progress, one must assume that what is private is also public in two senses of these words: that one's privacy (including sensitive matters) is rapidly corroded by the private sector and — that whatever it learns is also available to the government.