Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level

Laura Hildner[*]

Introduction: The Next Big Thing

It became known as the Broken Arrow Affair.[1] For four months in 2003, Wal-Mart equipped the shelves in a Broken Arrow, Oklahoma, store with a new technology capable of tracking the Max Factor Lipfinity lipstick containers stacked on them. Seven hundred and fifty miles away in Cincinnati, Procter & Gamble researchers detected when consumers removed lipsticks from the shelves. That action triggered a video monitor, which allowed the researchers to watch the consumers as they handled the lipstick.[2]

The technology that made this secret study possible is known as Radio Frequency Identification (RFID). RFID is a generic term for technologies that use radio waves to identify people or objects, and it has been described as "tech's official Next Big Thing."[3] RFID has been available since World War II, when the British army used it to recognize friendly aircraft,[4] and it is familiar to people in the northeastern United States as the

[*] J.D., Harvard Law School, 2005; A.B., Stanford University, 1999. I am grateful to Charles Nesson, Martha Minow, and Jonathan Zittrain for their comments on a draft of this Note. Thanks also to the members of the *Harvard Civil Rights-Civil Liberties Law Review* for their editorial guidance and for their fellowship throughout law school. Finally, I would like to thank my parents for serving as exemplary role models in the fields of law and education, and for inspiring me in countless other ways while providing endless support.

[1] The phrase "broken arrow" commonly refers to a missing nuclear weapon. *See, e.g.*, Wikipedia, *at* http://en.wikipedia.org/wiki/Broken_Arrow (last visited Nov. 20, 2005); Broken Arrow (20th Century Fox 1996) (depicting a U.S. army captain trying to stop a rogue major who has stolen a nuclear missile).

[2] Howard Wolinsky, *P&G, Wal-Mart Store Did Secret Test of RFID*, Chi. Sun-Times, Nov. 9, 2003, at 36.

[3] Staff of the Fed. Trade Comm'n, Radio Frequency Identification: Applications and Implications for Consumers 1 (2005), *available at* http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf (citing Jo Best, *Cheat Sheet: RFID*, Silicon.com, Apr. 16, 2004, http://www.hardware.silicon.com/storage/0,39024649,39120040,00.htm).

[4] *Radio Frequency Identification (RFID) Technology: What the Future Holds for Commerce, Security, and the Consumer: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of the House Comm. on Energy and Commerce*, 108th Cong. 10 (2004) [hereinafter *RFID Technology*] (statement of Sanjay Sarma, Associate Professor of Mechanical Engineering, Massachusetts Institute of Technology).

technology that enables the EZ-Pass toll payment system. Recently, RFID has been developed for use by manufacturers, distributors, and retailers.[5] Wal-Mart gave its 100 top suppliers until January 2005 to install RFID tags on product cases intended for three distribution centers in Texas, and the next 200 suppliers will adopt RFID by January 2006.[6] Wal-Mart's competitors, such as Target and Albertson's, have initiated their own RFID trials.[7] This momentum signals that RFID technology will become a common element of the products that American consumers buy.[8]

An RFID tag, the first element of RFID systems, is a silicon chip and antenna combination that can be attached to or incorporated into consumer goods. Tags can be three-tenths square millimeters, or as invisible as a grain of sand.[9] In retail environments, the chip contains an Electronic Product Code (EPC), which bears some resemblance to the bar codes currently imprinted on many consumer goods. A difference between bar codes and RFID chips is that bar codes contain only generic product information, whereas RFID chips are encrypted with a unique code that makes the products to which they are attached individually identifiable. The tags' antennae transmit the chips' particularized information to the second key component of RFID systems, the reader. Readers can be mobile or stationary and they vary in size and power; they use radio waves to scan tags for the data they possess. The tags considered for commercial uses do not have a battery and they operate at ultrahigh frequency, meaning readers can access them at a range between three and fifteen feet. Unlike bar code scanners, readers can receive information without being aimed at a tag or having a tagged item in their line of sight. They can also process multiple items at one time. Databases are the final important element of RFID systems. They receive the information programmed onto a tag from the reader and store and inter-

---

[5] "RFID technology is on the brink of widespread applications in manufacturing, distribution, retail, healthcare, safety, security, law enforcement, intellectual property protection and many other areas, including mundane applications like keeping track of personal possessions." *RFIDs and the Dawning Micro Monitoring Revolution*, 150 CONG. REC. S2990 (daily ed. Mar. 23, 2004) (remarks of Sen. Leahy at Georgetown University Law Center's conference on the legal and technological challenges of video surveillance). This Note focuses on retail applications.

[6] An oft-cited study suggested that only twenty-five percent of Wal-Mart's top suppliers would be on schedule by January 2005, but Simon Langford, manager of Wal-Mart's Global RFID strategy arm, said 108 suppliers will have complied by the end of January 2005. Christopher R. Yeich, *Wal-Mart's RFID Manager Bullish About Progress of Initiative*, 2 RFID PRODUCT NEWS 1 (2005), *available at* http://www.rfidproductnews.com/issues/2005.01/feature/bullish.php.

[7] Brian Dipert, *Reading Between the Lines: RFIDs Confront the Venerable Bar Code*, Oct. 14, 2004, at 54, *available at* http://www.edn.com/contents/images/468418.pdf.

[8] *RFID Technology*, *supra* note 4, at 6 (statement of Rep. Cubin). One hundred million consumers walk through the doors of Wal-Mart alone each week.

[9] *Hitachi Unveils Smallest RFID Chip*, RFID J., Mar. 14, 2003, http://www.rfidjournal.com/article/articleview/337/1/1.

pret it, linking the EPC to product information and potentially the individual product to the person who possesses it.[10]

Proponents of RFID technology believe one of its primary benefits is increased visibility into supply chains. Retailers lose between $180 billion and $300 billion annually because they have imprecise ability to maintain constant and accurate inventory data.[11] RFID readers provide automatic and continual information about the location and quantity of tagged goods as they proceed from the manufacturer to the distribution center, where they eliminate the need for manual counting and recounting, to the store. This helps retailers foresee and prevent shortages of high-demand goods or, alternatively, excess inventory. RFID technology can also ensure shipments intended for California are not diverted to New York, spot instances of theft and allow them to be controlled in real time, and increase retailers' ability to identify counterfeit products. In addition, it allows retailers to conduct product recalls more efficiently and effectively.[12]

Retailers' dependence on supply chain logistics means that much RFID spending, which amounted to $1 billion in 2004 and is expected to grow to $4.6 billion by 2007, has initially been focused on backroom warehouses and distribution centers, not on store shelves.[13] Many of RFID's potential benefits can be achieved by tagging shipping cases and pallets of goods containing many items, rather than the individual products sold to consumers. However, for electronic items, such as televisions and computer equipment, and large products, like lawn mowers and bicycles, the shipping case often doubles as packaging, meaning tags employed for supply chain purposes end up in the hands of consumers.[14] Customers who bought Hewlett-Packard photo printers and scanners in Wal-Mart stores participating in RFID trials, for example, took live RFID tags home with them.[15] Also, uses of RFID technology more sophisticated than supply chain management specifically require item-level tagging. These include preventing shoplifting, pinpointing expired and defective goods, replacing cashiers with automatic systems that instantly register a cart worth of purchases, and digitally coding receipts for paperless returns and warranty claims. "In answer to a question . . . about whether Coca-Cola is *really* interested in uniquely identifying a single can of Coke among billions,

---

[10] STAFF OF THE FED. TRADE COMM'N, *supra* note 3, at 2–7.

[11] *See* Britt Wood, Senior Vice President for Indus. Relations, Retail Indus. Leaders Ass'n, Remarks at Fed. Trade Comm'n Workshop: Radio Frequency Identification (June 21, 2004), *available at* http://www.ftc.gov/bcp/workshops/rfid/transcript.pdf.

[12] *Id.*

[13] Sarah Lacy, *Inching Toward the RFID Revolution*, BUS. WK. ONLINE, Aug. 31, 2004, http://www.businessweek.com/technology/content/aug2004/tc20040831_4930_tc172.htm.

[14] These examples were taken from the congressional testimony of Wal-Mart's Chief Information Officer Linda Dillman. *RFID Technology*, *supra* note 4, at 17.

[15] Michael Garry, *The Privacy Hurdle; Like Loyalty Cards, RFID Tags Raise Questions About Consumer Privacy, Once Again Putting Retailers on the Spot*, SUPERMARKET NEWS, Nov. 15, 2004, at 67, 67.

Michael [Okoroafor, in charge of technical solutions for Coca-Cola] replied with a resounding *'YES'!*"[16]

The possibility of paperless returns and shelves always full with sought-after items suggests that some of the benefits of item-level tagging will accrue to consumers. A Prada store in New York City offers a consumer-friendly RFID experience; it tracks the RFID tags on clothing selected by customers in order to display related accessories on nearby screens.[17] RFID also promises exciting new possibilities such as "microwave ovens that can read the tags on packages and cook food without explicit instructions, refrigerators that can recognize expired foodstuffs, and closets that can tally their contents."[18] Yet along with these conveniences come profound privacy concerns.[19] The tagging of cases and pallets moving through the supply chain is relatively uncontroversial, but when those tags appear on the sales floor in goods sold to consumers, they permit retailers and third parties with RFID readers to profile consumers' choices and track their movements both inside and outside of the store without their knowledge or consent.

After learning of Wal-Mart's experiment observing women interact with tagged lipsticks in Broken Arrow, privacy advocates immediately denounced the study as evidence of retailers' willingness to abuse RFID technology at the expense of consumer privacy. "The trial is a perfect illustration of how easy it is to set up a secret RFID infrastructure and use it to spy on people," said Katherine Albrecht, Director of the United States-based group Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN).[20] Days after a *Chicago Sun-Times* reporter first publicized the Broken Arrow Affair, thirty-five consumer privacy and civil

---

[16] Katherine Albrecht, Director, Consumers Against Supermarket Privacy Invasion & Numbering, Address at the Harvard Journal of Law & Technology Symposium: RFID: Technological Innovation and Legal Responses (Apr. 22, 2005) (quoting Michael Okoroafor).

[17] The Prada RFID experiment is not completely successful because employee and consumer apathy has led to the technology going largely unused, but other clothing retailers, such as Abercrombie & Fitch, plan to launch new RFID stores. Jerry Brito, *Relax Don't Do It: Why RFID Privacy Concerns are Exaggerated and Legislation is Premature*, 2004 UCLA J.L. & TECH. 5 (2004).

[18] Ari Juels et al., *The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*, Proceedings of the 10th ACM Conference on Computer and Communications Security, Oct. 2003, at 103.

[19] Related to privacy is security. Security deals with the reality that data, once gathered, may be obtained by unauthorized parties such as computer hackers. Because the security concerns that pertain to RFID tend not to be unique to the technology but rather to plague all database systems, they are not the subject of this Note. *See* Ari Juels, *Technological Approaches to the RFID Problem*, *in* RFID: APPLICATIONS, SECURITY, AND PRIVACY 329, 339 (Simson Garfinkel & Beth Rosenberg eds., 2005).

[20] *Wal-Mart, P&G Involved in Secret RFID Testing: American Consumers Used as Guinea Pigs for Controversial Technology*, SPYCHIPS.COM, Nov. 10, 2003, http://www.spychips.com/press-releases/broken_arrow.htm; *see also* Andy McCue, *Gillette Shrugs off RFID-Tracking Fears*, NEWS.COM, Aug. 14, 2003, http://news.com/Gillette+shrugs+off+RFID-tracking+fears/2100-1039_3-5063990.html.

liberties organizations, including the American Civil Liberties Union (ACLU), the Center for Democracy & Technology (CDT), the Electronic Frontier Foundation (EFF) and the Electronic Privacy Information Center (EPIC), released a position paper addressing the threat that RFID technology poses to individual privacy.[21] They called for manufacturers and retailers to agree to a voluntary moratorium on item-level RFID tagging of consumer items until a formal technology assessment could occur. They also declared that some uses of RFID technology, such as coercing customers into accepting live or dormant RFID tags in the products they buy, are incompatible with a free society and should be banned.[22] Wal-Mart responded to the scandal defensively, first by denying that the Broken Arrow study had been done, and then by downplaying the privacy invasion it entailed.[23] Kevin Ashton, executive director of the Auto-ID Center, a partnership based at MIT between academic researchers and corporations like Wal-Mart, said: "I think that the idea that someone's privacy is at stake because there are a few RFID tags in a few lipsticks in one store is silly."[24] Privacy advocates and industry retailers thus demonstrated sharp disagreement over RFID, with privacy advocates accusing retailers of using the technology for surveillance purposes and retailers labeling the privacy advocates' claims as "misleading" and saying they had no intention to track consumers.[25]

Despite the acrimony and distrust between retailers and privacy advocates, in the congressional hearings, agency workshops, and press releases that followed the Broken Arrow Affair, the two groups agreed upon surprisingly similar approaches to the privacy issues posed by RFID. They both focused on national solutions for consistency, and both prioritized comprehensive, or baseline, privacy principles over technology-specific mandates.[26] The key difference is that privacy advocates are willing to have these emphases translated into federal legislation whereas industry forces favor self-regulation. An example of how industry representatives' and privacy advocates' mindsets nevertheless converge is that each side expresses distaste for where the RFID legislative action currently resides:

---

[21] Consumers Against Supermarket Privacy Invasion and Numbering et al., *RFID Position Statement of Consumer Privacy and Civil Liberties Organizations*, PRIVACY RTS. CLEARINGHOUSE, Nov. 20, 2003, http://www.privacyrights.org/ar/RFIDposition.htm [hereinafter CASPIAN et al.].

[22] *Id.*

[23] Wal-Mart spokespeople say there was a sign at the Broken Arrow store notifying consumers that there was a test in progress. *See RFID: Is it a Threat to People's Privacy? Lawmakers Act to Restrict Use of the Devices in Stores, While Retailers Question the Need for Legislation*, WOMEN'S WEAR DAILY, May 12, 2004, at 13.

[24] Wolinsky, *supra* note 2 at 36.

[25] The debate became sufficiently rancorous that the Grocery Manufacturers of America (GMA) attempted to obtain activist Katherine Albrecht's biography to see, according to an internal GMA e-mail, if she had a "juicy past" that they could use against her. ROBERT O'HARROW, JR., NO PLACE TO HIDE 288–89 (2005).

[26] *See supra* notes 20–25 and accompanying text.

state privacy proposals. Privacy bills regulating RFID were introduced in nine state legislatures in 2005.[27] Most required the labeling of RFID-tagged products. Some provided for the removal of tags and for limitations on businesses' ability to link tag identifications with consumers' personal data. These bills represent everything both sides agree is suboptimal: immediate legislation at the state level that targets a particular technology.

Industry representatives' and privacy advocates' common rhetoric poses problems for those concerned about the implications of item-level RFID tagging for consumers because it supports preserving the current legal regime, in which there are few federal or state restraints on RFID usage. In making privacy in general the issue rather than RFID specifically, privacy advocates intend to call attention to the many ways in which businesses invade consumer privacy and to combat multiple injuries simultaneously. The portrayal of RFID technology as just one imposition on consumers on par with others, however, encourages regulators to dismiss it as not uniquely threatening. That viewpoint justifies the Federal Trade Commission's recent decision to allow RFID users to self-regulate. Meanwhile, the baseline privacy legislation heralded by privacy advocates as the preferred alternative to self-regulation remains unrealistic; it is a political impossibility in a conservative presidential administration and it runs contrary to the United States' historical approach to privacy law. A further flaw of baseline privacy legislation is that it would meaningfully restrict the use but not the collection of personal information obtained through RFID; it thereby fails to erect an important barrier to the profiling and tracking of consumers. By framing their positions in terms that can be marshaled to support the lack of any privacy legislation and responding with a baseline solution that is politically infeasible and otherwise incomplete, the privacy advocates, who are supposed to be the voice of consumers in an arena where it is difficult for individuals to enforce their own privacy preferences, are leaving consumers stranded.

What is required is for privacy advocates to devote their attention to supporting the technology-specific state legislative proposals that they are currently neglecting. Part I of this Note argues that RFID technology poses a distinct and significant threat to consumer privacy even in a society where private entities routinely intrude upon individuals. It also addresses why, if RFID is so threatening, its usage is not covered by exist-

---

[27] Maryland, Massachusetts, Missouri, Nevada, New Hampshire, New Mexico, South Dakota, Tennessee, and Virginia. *See* H.D. 354, 419th Gen. Assem., Reg. Sess. (Md. 2005); H.R. 1447, 184th Gen. Ct., Reg. Sess. (Mass. 2005); S.R. 181, 184th Gen. Ct., Reg. Sess. (Mass. 2005); S.R. 128, 93rd Gen. Assem., 1st Reg. Sess. (Mo. 2005); A.R. 264, 73rd Gen. Assem., Reg. Sess. (Nev. 2005); H.R. 203, 159th Gen. Ct., Reg. Sess. (N.H. 2005); H.R. 215, 47th Leg., 1st Reg. Sess. (N.M. 2005); H.R. 1136, 80th Legis. Assem., Reg. Sess. (S.D. 2005); H.R. 1114, 80th Legis. Assem., Reg. Sess. (S.D. 2005); H.R. 300, 104th Gen. Assem., Reg. Sess. (Tenn. 2005); S.R. 699, 104th Gen. Assem., Reg. Sess. (Tenn. 2005); and H.R. 1304, 2004 Sess. (Va. 2004).

ing federal and state law. Part II explores various means of protecting consumer privacy from abuses of RFID, namely self-regulation, technology, and legislation, and explains why legislation in particular is a necessary component of any RFID privacy solution. This Part then investigates how retailers and privacy advocates, who seem to have fundamentally different interests with respect to consumer privacy, came to agree upon national, technology-neutral approaches to RFID, even if they disagree about the role of legislation in enforcing that approach. Part III demonstrates the consequences of this shared mindset and critiques baseline privacy law as the sole redress for RFID privacy violations, both in terms of its political feasibility and the degree of protection it affords. This Part subsequently outlines the benefits offered by technology-specific legislation as a supplemental strategy, offering a rubric for deciding when such legislation might be appropriate for a new technology. These benefits include providing consumer insight into a complicated technology, restoring an element of consumer choice in RFID contexts, and protecting consumer rights in an enforceable manner. This Part also shows why technology-specific legislation is not as rigid an approach as retailers and privacy advocates both fear. The Note finishes by explaining why lobbying for technology-specific legislation is best done at the state level and by detailing the provisions effective state legislation might entail. The Note ultimately reminds privacy advocates that privacy protection is a multi-layered effort. Technology-neutral and technology-specific regulations are not solutions to be argued in the alternative, but remain mutually reinforcing possibilities.

I. The Nature of the Arrow

A. RFID's Distinguishing Characteristics

The United States is arguably becoming a surveillance society.[28] High-tech ways of invading people's privacy, from implantable microchips to data-mining, are proliferating. The explosion of these technologies, along with computers, cameras, sensors, wireless communications, GPS, and biometrics, means that there are few technical barriers to establishing an Orwellian Big Brother regime in the private sector.[29] RFID technology helps vaporize those that remain by streamlining consumer profiling and tracking to an unprecedented degree.[30]

---

[28] *See generally* O'Harrow, *supra* note 25.

[29] Jay Stanley & Barry Steinhardt, ACLU Tech. & Liberty Program, Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society 1 (2003), http://www.aclu.org/Files/OpenFile.cfm?id=11572.

[30] Information about consumers' locations is available to their wireless service providers, but such providers, unlike retailers, are centralized and federally regulated data-gatherers. Third parties with special purpose equipment could track consumers through their mobile phones, but that would require expertise and investment. RFID is arguably a more significant

RFID receives so much attention from privacy advocates because the cues that alert people to intrusions into their privacy and allow them to mitigate those invasions are non-existent in its realm. RFID operates invisibly. Retailers may incorporate tags into products without the knowledge of the individual who obtains them. Tags are promiscuous in that they can communicate with any reader; readers can be implanted in floor tiles, carpeting, and doorways, in addition to retail shelving and counters. They can scan tags at a distance, through purses, shopping bags, suitcases, and even walls, making it impossible for a consumer to detect when she is being monitored.[31] While the data on the tag may be no more than an EPC serial number, an interested party with access to the appropriate database—for example, one recording credit card purchases—could link an item to the owner's name and profile. The result is that people become identifiable through their possessions.[32]

Some commentators minimize the significance of RFID technology by remarking that RFID is but one of many data-gathering techniques and that the data it accesses can be collected through other means.[33] This argument ignores the special ability of RFID to operate free from consumer consent. The stealth nature of RFID distinguishes it from technologies that can only intrude upon consumer privacy after consumers make the conscious choice to interact with them. For example, supermarket loyalty programs require customers to swipe their discount cards and online shopping necessitates completing and submitting a website form.[34] Unfettered use of RFID technology eliminates the element of consumer consent; monitoring may occur whether or not a consumer acquiesces or even is aware that information is being collected.[35] The argument that RFID is

---

threat to privacy than mobile phones because readers will be "readily available and ubiquitously deployed." RSA Security, *FAQ on RFID and RFID Privacy*, http://www.rsasecurity.com/rsalabs/node.asp?id=2120 (last visited Nov. 20, 2005). In addition, Senator Leahy has stated:

> RFID chips are more powerful than today's video surveillance technology. RFIDs are more reliable, they are 100 percent automatic, and they are likely to become more pervasive because they are significantly less expensive, and there are many business advantages to using them. RFIDs seem poised to become the catalyst that will launch the age of micro-monitoring.

RFIDs and the Dawning Micro Monitoring Revolution, 150 CONG. REC. S2989 (daily ed. Mar. 23, 2004) (remarks of Sen. Leahy).

[31] CASPIAN et al., *supra* note 21.

[32] *Id.*

[33] *See* Thomas Claburn, *RFID Is Not the Real Issue*, INFO. WK., Sept. 15, 2004, http://www.informationweek.com/showArticle.jhtml?articleID=47204120.

[34] This comparison is not meant to diminish concerns about online privacy. Websites track not only the purchases consumers make, but the pages they view, for how long and in what order. The sale of such personal information has become a source of revenue for Internet ventures, thus allowing consumers' viewing habits to be made available to parties beyond those of which they may have conceived.

[35] *See* Dipert, *supra* note 7, at 52.

not distinct also ignores how fine-grained a level of data collection RFID permits. An RFID reader can not only determine that a person bought a book, but can also distinguish that book from all other copies of the book in the world.

Even if the information RFID collects could be wholly gathered through alternative means, RFID remains significant from a privacy standpoint for automating the information collection and storage process.[36] Professor Jonathan Weinberg imagines efforts to track the movement of automobiles down a highway. Nothing prevents a person from standing on the side of the road and copying down license plate numbers or photographing them with a camera. That process, however, is time-consuming and it is expensive to enter the information gathered into a digital database. The result is that such information is not in fact digitally collected. Position an RFID reader alongside a highway, however, and it can collect data from RFID tags in automobile tires. Link that tag data to automobile VINs in a database, and identifying whose cars proceed down the highway and including that information in a searchable database becomes a fully automated process, cheap and easy to accomplish. Weinberg concludes: "the less it costs to collect, store, and analyze information, the more information will in fact be collected, stored, and analyzed."[37]

The privacy intrusions that could result from RFID-tagging of consumer goods include profiling, surveillance, and targeted action.[38] First, a network of readers could collect RFID information from consumers' belongings and use it to establish or add to consumers' dossiers. The invasion would be greatest when the person or entity in control of the reader could relate the consumers' RFID tags to personally identifying information through a database. Most retailers would be able to do that by determining whose credit card purchased the item; in turn, third parties could buy such information. Even without being able to associate an RFID tag with a name, however, someone with a reader can compile data about a person over time. Tags are unique and semi-persistent identifiers that can indicate that "this is the same guy who was here making trouble last week."[39] They can divulge a surprisingly complete profile of a person simply by revealing the products that the person carries. Over-the-counter medicines expose health conditions; certain foods, such as kosher products, indicate religious affiliation; books suggest political allegiances and life-

---

[36] Jonathan Weinberg, *RFID, Privacy and Regulation*, *in* RFID: APPLICATIONS, SECURITY, AND PRIVACY, *supra* note 19, at 83, 90.

[37] *Id.*

[38] *Id.* at 91. Abuses of the personal data collected through RFID systems might include blacklisting, witch hunts, ex ante discrimination and guilt prediction, unknown accusations and accusers, and denial of due process, as well as a number of criminal activities. A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV 1461, 1471–72 (2000) (describing the dangers of "dataveillance").

[39] Weinberg, *supra* note 36, at 89.

style choices.[40] Social networks can be determined through correlation.[41] Second, readers are capable of disclosing how consumers move through space. This does not require RFID readers to be placed every few feet; to track an individual's whereabouts in a town, readers need only be present at select locations such as building entrances.[42] Third, the combined knowledge of consumers' characteristics and location allows businesses to target consumers for differential treatment. IBM, for example, has developed a product that relies upon doorway RFID readers to identify high net-worth individuals as they enter financial institutions so they can be signaled out for personal service. Similar systems might appeal to restaurant and boutique owners and nefarious discrimination thereby seems possible.[43]

The data collectors in these scenarios may be retailers, but given the small size and decreasing expense of readers and the incentives retailers have to sell database information, they could become nearly anyone else. Retailers argue that they have little motivation to invade their customers' privacy, and that uses of RFID that, for example, identify customers by their clothing and market to them by name, are more likely to alienate customers than impress them.[44] While certain forms of direct marketing may be too obviously creepy, other means of profiling and surveillance will align with retailers' profit motive. Businesses have a strong incentive to learn as much about consumers as possible so that they can target those who are most lucrative. Loyalty programs and detailed product registration forms have proliferated precisely because they present a means of gathering information about consumers.[45] As Congressman Cliff Stearns (R-Fla.) said during House hearings on RFID: "We are told that suppliers and retailers aren't interested in doing the kind of surveillance about which I am concerned, yet the example at Wal-Mart [in Broken Arrow] leads me to believe there may be an interest."[46] The possibility of synergies creates reasons for retailers to share the personally identifiable information they have compiled with others (and this is especially true because they are not likely to get caught sharing). Third parties likewise have their own reasons for acquiring it. The pastor in Kennedale, Texas,

---

[40] Robert Ellis Smith & Mikhail Zolikoff, *Citizens: Getting at Our Real Concerns*, *in* RFID: APPLICATIONS, SECURITY, AND PRIVACY, *supra* note 19, at 413, 415–16.

[41] David Bender, *Data Protection: Three "Hot Topics," in* PLI's TENTH ANNUAL INSTITUTE FOR INTELLECTUAL PROPERTY LAW 11, 70 (PLI Pats., Copyrights, Trademarks, and Literary Prop. Course, Handbook Series No. 2909, 2004), WL 801 PLI/Pat 11.

[42] CASPIAN et al., *supra* note 21.

[43] Katherine Albrecht, *RFID: The Doomsday Scenario*, *in* RFID: APPLICATIONS, SECURITY, AND PRIVACY, *supra* note 19, at 259, 263.

[44] *See* Jerry Brito, *supra* note 17. *Cf.* Roberta A. Fusaro, *None of Our Business*, HARV. BUS. REV., Dec. 2004, at 33 (presenting case study of clothing manufacturer considering implanting RFID tags in popular visors so manufacturer could then market directly to the visor-wearing teenagers who frequent its stores).

[45] Stanley & Steinhardt, *supra* note 29, at 4 (discussing the commoditization of personal information).

[46] *RFID Technology*, *supra* note 4, at 4.

who took photographs of cars parked in pornography vendors' parking lots and then mailed invitations to attend his church to the cars' registered owners, would likely find himself interested in RFID.[47] What he would require is for his targets to carry something with a live RFID tag and for him to have a reader in close proximity and access to a database that linked a name to the tag.

B. RFID Under the Law

As Justice Black wrote in *Griswold v. Connecticut*, privacy is "a broad, *abstract and ambiguous concept.*"[48] The word privacy is not explicitly mentioned in the U.S. Constitution, but as the Supreme Court recognized in *Griswold*, privacy is nevertheless entangled with the liberties and freedoms that the Constitution affords to American citizens. Privacy has traditionally been discussed in the United States as the right to be free from unreasonable search and seizure or intrusion, and the right to protect personal information.[49] Other definitions of privacy include the right of anonymity and the right to be left alone. The scanning of individuals carrying RFID-tagged goods, and consequently the obtaining of knowledge regarding those persons' preferences, characteristics, whereabouts, and identities, implicates privacy rights in their several forms.

Given the privacy threat posed by RFID, it may seem odd that there is no body of law in the United States that governs RFID-tagging of consumer goods. One reason, suggested by Professor Martha Minow, is that American law

> [A]ssumes and enforces a distinction between the public and the private sphere . . . . The United States Constitution makes state action a prior requirement for most constitutional provisions affecting liberty, and it is within the concept of liberty that courts tend to identify privacy. State action is required to trigger the protections of freedoms of speech, religion, and assembly, [and] the right to be secure against unreasonable searches and seizures.[50]

---

[47] NBC 5 News, *Pastor Brings Porn Fight to Mayor's Office*, http://www.nbc5i.com/news/3369257/detail.html (last visited Nov. 19, 2005).

[48] 381 U.S. 479, 509 (1965) (Black, J., dissenting).

[49] Stephanie Perrin, *RFID and Global Privacy Policy*, *in* RFID: APPLICATIONS, SECURITY, AND PRIVACY, *supra* note 19, at 57, 58.

[50] Peter Galison & Martha Minow, *Our Privacy, Ourselves in the Age of Technological Intrusions*, *in* HUMAN RIGHTS IN THE WAR ON TERROR 258, 258–94 (Richard Wilson ed., 2005). The authors remind us that when data collected by retailers is made available for sale to the government, the government can evade the state action requirements which would have attached if the government had pursued the information directly. The government's relationship to RFID technology raises privacy concerns at least as serious as those preva-

Under this jurisprudence, the marketplace is considered private and is left under-protected.

Congress has gone beyond the Constitution to pass statutes that preserve privacy in the absence of state action, but in doing so, it has taken a stop-gap, industry-focused approach that has left substantial holes.[51] A survey of the United States' privacy laws led Professor James Nehf to conclude: "[P]rivacy in the non-governmental sector has been treated primarily as a commercial policy problem rather than one of ensuring fundamental individual rights or civil liberties."[52] Legislators' discomfort over the disclosure of Judge Robert Bork's video rental selections during his Supreme Court confirmation hearings led to video records being protected by a strong privacy law while many other sectors of the economy remained unregulated.[53] For those statutes that have passed, Congress has often allowed lobbying groups to secure limitations that partially vitiate the statutes' goal of protecting individual privacy. A recent example of this phenomenon is the Graham-Leach-Bliley Act of 1999,[54] which covers the financial services industry only and provides consumers with opt-out rights when financial institutions seek to disclose their personal data to other companies. The practical result of a default position in favor of sharing is that most consumer information is available for distribution; consumers either do not understand what is at stake or do not have the will to navigate densely written release forms.[55] This is typical of a privacy framework in which "the limitation of constitutional analysis, the vagaries of statutory coverage, and the frailty of individual vigilance, taken together, expose personal privacy to massive challenge by corporate and market activities."[56]

Absent legislation, the Federal Trade Commission (FTC) may exercise some control over RFID. The FTC announced in March 2005 that it will presently refrain from issuing guidelines regarding RFID and instead

---

lent in the marketplace and is the subject of other publications, such as, O'HARROW, *supra* note 25.

[51] For examples of federal laws that take an industry-sector approach to protecting privacy, see the Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681–1681t (2000) (providing citizens with rights regarding the use and disclosure of their personal information by credit reporting acts); Privacy Act of 1974, 5 U.S.C. § 552a (2000) (providing individuals with rights concerning their personal information in government records systems); Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (2000) (protecting the privacy of school records); Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (2000) (mandating privacy protection for records maintained by cable companies); Video Privacy Protection Act of 1991, 47 U.S.C. § 227 (2000) (protecting the privacy of videotape rental information). For an overview of federal privacy law, see DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 22–25 (2003).

[52] James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. COLO. L. REV. 1, 4–5 (2005).

[53] *See id.* at 9–10.

[54] 15 U.S.C. §§ 6801–6809 (2000).

[55] Galison & Minow, *supra* note 50, at 276.

[56] *Id*.

it will allow companies using RFID to regulate themselves regarding matters of consumer privacy.[57] Still, section 5 of the Federal Trade Commission Act[58] prohibits deceptive or unfair acts or practices in or affecting commerce. The FTC has used this authority on behalf of consumers in prosecuting companies that have violated their own privacy policies.[59] FTC Chairman Deborah Marjoras has stated, "If a company's privacy policy materially misstated how the company used RFID to collect information about consumers, the commission could bring an enforcement action."[60] Thus, if a retailer promises that it will place labels on all goods containing RFID tags and it fails to do so, the FTC can order the retailer to comply and, if necessary, can seek judicial intervention.

FTC prosecution does not provide significant protection in RFID contexts because the FTC's authority is discretionary: the agency has limited resources, and it may refrain from pursing many of the violations reported to it. Moreover, the FTC's standard enforcement procedure is to investigate charges carefully and to negotiate with the transgressor a reprimand and promise to reform. Such a prolonged process is not suited to stopping the transmission of sensitive personal information into unauthorized channels. Lastly, and perhaps most importantly, the FTC cannot prosecute a company unless that company has voluntarily undertaken the affirmative step of establishing a privacy policy that subjects it to the agency's jurisdiction. If a company simply avoids making any statements about its privacy policies, it can implement RFID systems as it deems appropriate.[61] The FTC has not taken any enforcement actions against companies based on their use of RFID technology to date, nor has it monitored which are using RFID technology.[62]

---

[57] Jonathan Collins, *FTC Asks RFID Users to Self-Regulate*, RFID J., Mar. 10, 2005, http://www.rfidjournal.com/article/view/1437/1/1/.

[58] 15 U.S.C. § 45 (2000).

[59] *See, e.g.*, Petco Animal Supplies, Inc., No. C-4133 (Fed. Trade Comm'n Mar. 4, 2005) (final dec. and order), http://www.ftc.gov/os/caselist/0323221/00308do0323221.pdf (placed on the public record Nov. 17, 2004) (enforcing section 5 and resolving Commission claims that Petco had violated its own privacy policy—and federal law—by failing to take reasonable or appropriate measures to prevent commonly known attacks by hackers). Other examples *available at* http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

[60] Claire Swedberg, *FTC Readies an RFID Report*, RFID J., Oct. 5, 2004, http://www.rfidjournal.com/article/view/1151/1/1/.

[61] Doug Campbell, *RFID and the United States Regulatory Landscape*, *in* RFID: APPLICATIONS, SECURITY, AND PRIVACY, *supra* note 19, at 99, 124 (discussing these shortcomings of the FTC in implementing RFID privacy goals). For a creative argument that RFID implementation might be bound by the Electronic Communications Protection Act (ECPA), 18 U.S.C. §§ 2510–2522 (2000), that governs anyone improperly accessing electronic data, see Reuben R. Levary, et al., *RFID, Electronic Eavesdropping and the Law*, RFID J., Feb. 14, 2005, http://www.rfidjournal.com/ article/view/1401/1/82. *See also* Campbell, *supra*, at 124 n.35 (writing that the ECPA's "application to RFID is uncertain. It does not cover the gathering and use by an RFID user of data generated by its *own* system, which of course is the case with most planned consumer applications.").

[62] Swedberg, *supra* note 60.

Ten states have constitutionally guaranteed rights of personal privacy,[63] but as with federal constitutional protections, they are virtually always limited to governmental activities. Some commentators suggest that state common law privacy torts provide the missing constraint on abusive RFID practices.[64] A claim of unreasonable intrusion upon the seclusion of another might, for example, cover the surreptitious monitoring that RFID facilitates. The intrusion arguably meets the elements of being both "intentional[ ]" and "highly offensive to a reasonable person."[65] Even if this tort applies (though it generally does not when the individual targeted is in a public place),[66] it is not a practical option for protecting privacy at the individual, non-class-action level where attorneys' fees are not recoverable.[67] A meaningful solution to RFID privacy invasions would seek to prevent harm and not simply provide a means of redressing violations.[68] The reality is that there are few existing legal protections of consumer privacy against RFID, and tort law is no exception.[69]

II. Recovering the Arrow

A. Self-Regulatory and Technical Strategies for Addressing Consumer Privacy Concerns

Other than supplementing existing statutes with new legislation, the most oft-suggested solutions for addressing RFID privacy concerns are industry guidelines and technological solutions.[70] A self-regulatory system that is already in place is EPCglobal, a nonprofit joint venture between EAN International and the Uniform Commercial Council, the two organizations that currently administer the barcode. EPCglobal's 400 members include retailers like Wal-Mart and consumer products vendors like Gillette and Proctor & Gamble. They have tasked EPCglobal with finalizing the worldwide standards governing, for example the type of RFID tags to be used, with the aim of facilitating RFID's adoption. EPCglobal simultaneously directs its members' privacy practices. The group's non-binding

---

[63] They are Alaska (art. I, § 22); Arizona (art. II, § 8); California (art. I, § 1); Florida (art. I, § 12); Hawaii (art. I, §§ 6–7); Illinois (art. I, §§ 6, 12); Louisiana (art. I, § 5); Montana (art. II, §10); South Carolina (art. I, § 10); and Washington (art. I, § 7). An overview of state constitutional privacy protections is available through the National Conference of State Legislatures *at* http://www.ncsl.org/programs/lis/privacy/stateconstpriv03.htm (last visited Nov. 19, 2005).

[64] *See* Brito, *supra* note 17; Jim Harper, *RFID Tags and Privacy: How Bar-Codes-on-Steroids Are Really a 98-Lb. Weakling*, 89 CEI OnPoint, 10–12 (2004).

[65] Restatement (Second) of Torts § 652B (1977).

[66] *See id*. at § 652B cmt. c.

[67] Campbell, *supra* note 61, at 119 n.32.

[68] *Id*.

[69] For examples of how privacy lawyers are advising their clients to handle RFID implementations in this legal landscape, see Harry A. Valetk, *Is Radio Frequency ID Technology Watching You?*, Legal Times, Dec. 6, 2004, at 17.

[70] *See, e.g.*, Staff of the Fed. Trade Comm'n, *supra* note 3, at 16–17.

"Guidelines on EPC for Consumer Products" encourage consumer notice, choice, and education as well as certain record use, retention, and security practices.[71] The Guidelines are explicitly tentative: they will "evolve as [RFID] applications are developed and implemented."[72] The current Guidelines advise companies engaged in "large-scale deployment" of RFID to give consumers clear notice of the presence of RFID technology and to inform them of whatever choice that they have to discard, disable, or remove RFID tags.[73] EPCglobal anticipates that for most products its tags will be part of the product's packaging or otherwise disposable. The Guidelines do not address the creation of personally identifiable data, leaving its collection and mining to "all applicable laws." EPCglobal's sole means of prompting compliance is to provide a forum for companies and consumers to address uses of RFID that are inconsistent with the Guidelines.[74]

Technology that interferes with RFID data-gathering processes has been devised to protect consumer privacy, and the emerging options offer attendant attractions and drawbacks.[75] One technological approach involves "blocker tags." Consumers can place blocker tags in the vicinity of RFID tags to overwhelm readers by making them believe each RFID tag contains all possible serial numbers. This "spamming" prevents readers from extracting the data on RFID chips. Consumers remain in control of which items they want blocked and when, and that allows them to benefit from potential, post-purchase applications of RFID, such as "smart" microwaves. Privacy advocates have criticized blocker tags for burdening consumers by forcing them to opt-in to privacy protection by purchasing blocker tags, and for creating two classes of consumers, those with blocker tags and those without.[76] Privacy advocates also fear that blocker tags could be defeated by other technologies, and they hence argue blocker tags provide consumers with a false sense of security. Retailers dislike blocker tags because they can be used by shoplifters to by-pass stores' security systems. A modified "soft blocker" technology permits consumers to alter the code on their RFID tags in accordance with their expressed privacy preferences at the point-of-sale. The tags will remain active for designated post-sale purposes, but inaccessible to other readers, thereby re-

---

[71] Guidelines on EPC for Consumer Products, http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html (last visited Nov. 19, 2005).

[72] *Id.*

[73] Wal-Mart adheres to the EPCglobal Guidelines in its RFID trials. *RFID Technology*, *supra* note 4, at 17 (statement of Linda Dillman, Executive Vice President and Chief Information Officer, Wal-Mart Stores, Inc.).

[74] For a critique of EPC Guidelines as they are currently phrased and recommendations for making them more robust using licensing mechanisms, see Campbell, *supra* note 67, at 130.

[75] Juels et al., *supra* note 18, at 332–39 (discussing how RFID tags can incorporate privacy-protecting technologies).

[76] CASPIAN et al., *supra* note 21.

ducing the ability of unauthorized parties to scan consumers surreptitiously. "Kill switches" are available too that permanently disable RFID tags at checkout. The kill process could be a cumbersome one for consumers, however, if retailers require them to wait in one line to purchase their goods and another to deactivate their RFID tags. Privacy advocates worry that retailers could use such delays to discourage consumers from disabling their tags. The effectiveness of "kill switch" technology also depends on whether retailers disclose that RFID tags are attached to products; consumers have to be aware of tags before they seek to deactivate them.[77]

The existence of self-regulatory and technological options does not obviate the need to consider legislative solutions. Self-regulation is desirable, but it has no binding force. It therefore produces uneven results that undermine its value. Sandy Hughes, Proctor & Gamble's global privacy executive, acknowledges that the EPCglobal Guidelines mask a lack of industry consensus on privacy policy.[78] Each company's decision to abide by the Guidelines may change suddenly in response to turnover in management, competitive positioning, or financial pressures, and thus lacks long-term credibility.[79] Even if there is consensus and good faith among industry participants, the limitations they impose on themselves may not address reasonable consumer concerns, but only those concerns CEOs think are justified.[80] Technology is likewise an incomplete source of privacy protection. It can restrict access to personal information in degrees, but it cannot create the desire for its own use, nor does technology contribute much to the protection of privacy after data has been collected.[81] Though the proponents of various approaches to consumer privacy often argue them in the alternative, only a mix of market, technological, and legal strategies has a realistic chance of confining privacy invasions.[82] Law can be evaded and it is difficult to design legislation that perfectly reconciles the sometimes competing interests of convenience and privacy. Still, law's ability to establish enforceable barriers to privacy invasions makes it a powerful contributor to consumer privacy.

---

[77] STAFF OF THE FED. TRADE COMM'N, *supra* note 3, at 21.

[78] *Tagging Privacy onto RFIDs*, PRIVACY LAWS & BUS., Jan.-Feb. 2004, at 19, 19, *available at* http://www.pandg.com/company/our_commitment/privacy_epc/Issue_71_PLB_International_Jan-Feb_2004.pdf.

[79] *See RFID Technology*, *supra* note 4, at 18–19 (reprinting Wal-Mart's privacy policy, which explicitly reserves to Wal-Mart the right to change the policy at any time).

[80] Campbell, *supra* note 67, at 116–17.

[81] Galison & Minow, *supra* note 50, at 260–61.

[82] *Id*.

B. Legislative Options for Addressing Consumer Privacy Challenges

1. Industry's Recommended Approach

The goal of industry members is to achieve the benefits of RFID technology in the most economical fashion, and they perceive legislation as an added cost of implementing RFID. Retailers speak with one voice through trade associations like the Grocery Manufacturers of America (GMA), and the GMA clearly opposes regulating RFID. At a FTC June 2004 workshop on RFID's applications and implications for consumers, industry representatives argued that regulation is an ill-suited response to a rapidly evolving technology in its initial stages of deployment.[83] The idea is that legislation is at best premature and lawmakers would likely overreach, curb uses of RFID that do not threaten privacy, and prevent the technology's development.[84]

Industry advocates oppose both federal and state RFID legislation, but, in the words of the GMA, "[s]ince the currently-known benefits of the technology arise in interstate commerce, a patchwork of state regulations of RFID would be particularly problematic."[85] Inconsistent standards across the country would create confusion and expense, slowing the spread of RFID, complicating its design, and limiting its innovation. Elizabeth Avery, Vice President of Government Affairs for the GMA, even argues, "If we get a lot of different states adopting a lot of different regulations it could put a halt to this technology."[86] Retailers perceive RFID implementation to be a national, not a state, issue and want the ability to campaign against legislation at that level.

Retailers' opposition to federal and especially state legislation co-exists with an awareness that industry must address consumer privacy concerns through alternative means; otherwise, consumers will resist RFID implementation and lawmakers will intervene.[87] Retailers' first response is to downplay privacy fears as unfounded; they insist they will respect

---

[83] STAFF OF THE FED. TRADE COMM'N, *supra* note 3, at 20. See for example the comments by Mallory Duncan, Senior Vice President and General Counsel to the National Retail Association: "Unless we are aiming to arrest potential benefits, we shouldn't write laws in response to imagined difficulties." *Id.* at 146. Also, during the U.S. Department of Commerce's workshop entitled *RFID in 2005: Technology and Industry Perspectives*, industry representatives reportedly "chaffed at suggestions that retailers should notify buyers of RFID use, and most disagreed with the idea of allowing users to voluntarily turn off tags." Campbell, *supra* note 67, at 126 n.42.

[84] JULIE HUTTO & ROBERT D. ATKINSON, PROGRESSIVE POLICY INST., RADIO FREQUENCY IDENTIFICATION: LITTLE DEVICES MAKING BIG WAVES 7–8 (2004), *available at* http://www.ppionline.org/documents/RFID_1006.pdf.

[85] *RFID Technology*, *supra* note 4, at 68 (prepared statement of GMA).

[86] Steven Oberbeck, *RFIDs May Aid Inventory*, SALT LAKE TRIB., May 23, 2004, at E1.

[87] *RFID Technology*, *supra* note 4, at 67 (prepared statement of GMA) ("While EPC/RFID can produce major benefits, the technology also raises public policy issues that must be addressed in a proactive and responsible way. Chief among those issues are concerns about consumer privacy . . . .").

consumers' privacy because they have a profit incentive to please their customers.[88] They also argue that a read range of less than fifteen feet makes many privacy doomsday scenarios involving location tracking technically unlikely,[89] something privacy advocates vigorously dispute.[90] Retailers additionally emphasize the speculative nature of the privacy debate, claiming that widespread item-level tagging may never materialize. They focus on the fact that the cost of RFID tags would have to drop from their current price of a quarter to around five cents or a penny before it would become economically feasible to tag inexpensive goods like cereal boxes.[91] Finally, they suggest that even if privacy threats become a reality, self-regulation is an adequate response that is preferable to legislation. Self-regulation possesses the benefits of being quicker to craft and deploy, more adaptable to future developments, less restrictive of business practices, and less entangled with administrative costs.[92]

Though industry recognizes it must assuage consumers' RFID privacy concerns, industry would prefer not to discuss privacy in RFID-specific terms. Linda Dillman, Wal-Mart's chief information officer, reflected the industry's preference for contemplating consumer privacy in technology-neutral language during her July 2004 testimony before Congress: "[W]e absolutely support protection of private information, personal information, but we don't believe that data collected by RFID should be different. We believe there needs to be a standard for all personal information, no matter how it's collected."[93] Part of her justification was the inefficiency inherent in a retail environment where each data-gathering technology operates under different privacy standards. However, industry advocates' persistent efforts to equate RFID with other technologies with surveillance potential, such as cell phones and the Internet,[94] suggest a conscious attempt to portray RFID as simply another innovation whose privacy drawbacks consumers will accept in exchange for the conveniences offered. The hope, according to the anti-regulatory Progressive Policy Institute, is that if industry advocates can implement RFID before laws governing it are passed, "consumers will get used to RFID technology over time and will develop appropriate expectations about the level of privacy they have in stores."[95] Such acceptance would obviate the demand for legislation.

---

[88] *See* Jim Harper, *supra* note 64, at 7–9 (coinciding with the FTC hearing on RFID).

[89] *See generally* Campbell, *supra* note 67, at 116–19 (categorizing businesses' responses to consumers' RFID privacy concerns).

[90] *See* CASPIAN et al., *supra* note 21.

[91] *See RFID Technology*, *supra* note 4, at 17 (statement of Linda Dillman, Chief Information Officer, Wal-Mart). Analysts, however, say that RFID tags costing fifty cents justify tracking goods that cost fifteen dollars or more. *Benetton to Tag Fifteen Million Items*, RFID J., Mar. 12, 2003, http://www.rfidjournal.com/article/articleview/344/1/1.

[92] Campbell, *supra* note 67, at 130 n.44.

[93] *RFID Technology*, *supra* note 4, at 57.

[94] *Id*. at 68 (prepared statement of GMA).

[95] HUTTO & ATKINSON, *supra* note 84, at 5.

Industry advocates have substantial support at the federal level in their resistance to RFID-specific legislation. Federal policymakers explored RFID privacy issues during a June 2004 FTC workshop, entitled "Radio Frequency Identification: Applications and Implications for Consumers," and concluded that RFID users should self-regulate.[96] Industry representatives successfully persuaded FTC attorneys to see RFID as comparable to other technologies by which personal information is collected. Julie Brof, an FTC attorney who helped draft the report summarizing the agency's conclusions, reflected the technology-neutral terminology pressed by industry advocates when she said: "There is a realization that what we are talking about is largely database security and not just something specific to RFID."[97] In July 2004, the Subcommittee on Commerce, Trade, and Consumer Protection of the House Energy and Commerce Committee also held a hearing, "Radio Frequency Identification (RFID) Technology: What the Future Holds for Commerce, Security, and the Consumer."[98] Like the FTC workshop, it did not lead to formal action.

In Congress, only a handful of Democrats have expressed support for national RFID-specific legislation and Republicans with ties to industry have vocalized their opposition. In March 2004, Senator Leahy (D-Vt.) announced that he would consider advancing RFID-specific legislation,[99] and in June 2004, Representative Gerald Kleczka (D-Wis.) introduced the "Opt Out of ID Chips Act" in the House. The proposed legislation would have required the FTC to adopt rules that would ensure that businesses could not sell products with RFID tags unless (1) the product carried a warning label, and (2) the purchaser had the option of having the RFID tag removed or permanently disabled at time of sale.[100] The bill died in committee and has not been reintroduced. The anti-regulatory sentiment of President George W. Bush's second term has instead prevailed. In March 2005, the Senate Republican High Tech Task Force announced that one of its policy goals was to protect RFID from "premature regulation or legislation in search of a problem."[101] Given the FTC's preference for

---

[96] *See* STAFF OF THE FED. TRADE COMM'N, *supra* note 3.

[97] Jonathan Collins, *FTC Asks RFID Users to Self-Regulate*, RFID J., Mar. 10, 2005, http://www.rfidjournal.com/article/view/1437/1/1/. *See also* STAFF OF THE FED. TRADE COMM'N, *supra* note 3. Although this report says it represents the view of FTC staff, FTC Commissioners voted 5-0 to release it, suggesting comfort with its findings. Campbell, *supra* note 67, at 126 n.40.

[98] *See RFID Technology*, *supra* note 4.

[99] *See RFIDs and the Dawning Micro Monitoring Revolution*, *supra* note 5 and accompanying text.

[100] *Protect Personal Privacy by Notifying Consumers of the Presence of Tracking Devices in Everyday Items*, 150 CONG. REC. E1224 (daily ed. June 24, 2004) (statement of Rep. Kleczka).

[101] Press Release, Senate Republican High Tech Task Force, High Tech Task Force Unveils Policy Goals (Mar. 9, 2005), http://republican.senate.gov/httf/index.cfm?FuseAction=PressReleases.Detail&PressRelease_id=66. The purpose of the Senate Republican High Tech Task Force is to serve the Republican Leadership's outreaches to the technology community and to advise the Republican Caucus on technology issues. *Id.*

self-regulation, the lack of any RFID-specific legislation proposed in the current session of Congress, and the opposition expressed by the party in the majority, national legislation directly protecting consumers against RFID abuses is unlikely to be forthcoming absent a major scandal.

RFID-related laws have a more realistic chance of passage at the state level, where lawmakers have been active in drafting legislation and bringing it to a vote. In 2004, legislators in Maryland, Utah, Virginia, Missouri, and California introduced bills that sought to respond to the adoption of RFID technology in the consumer context.[102] In 2005, legislators in Maryland, Missouri, and Virginia reintroduced bills pertaining to RFID and lawmakers in Massachusetts, Nevada, New Hampshire, New Mexico, South Dakota, and Tennessee also sought RFID privacy legislation.

Thus far, no RFID privacy measure has passed through a state legislature. This is due in part to vigorous lobbying by industry groups committed to the idea that RFID-specific legislation is even more undesirable at the state level than at the federal level. In New Mexico, for example, lobbyists led by GMA were credited by Representative Mimi Stewart with persuading the House Judiciary Committee to table a "Radio Frequency Right to Know Bill."[103] The proposed legislation would have allowed businesses to use RFID inside a store or warehouse, but would have required them to disable or remove RFID tags once consumers purchased the attached products. In addition, each item with an RFID tag would have carried a label notifying consumers RFID was present, and businesses would not have been allowed to share with other businesses the information they gathered on consumers via RFID.[104] The bill sailed through its first committee with unanimous bipartisan support, but then opposition from business groups emerged.[105] These groups testified that RFID could save industry billions of dollars in the cost of tracking inventory and that any legislation that would, in the words of an EPCglobal representative, even "create an impression of restricting [RFID] would chill development."[106] Notably, most of the requirements in the New Mexico bill overlapped with the voluntary guidelines for RFID use developed by EPCglobal and with which its members ostensibly comply. Nonetheless, EPCglobal rep-

---

[102] Joshua Nelson & Nick Steidel, Nat'l Conf. of State Leg., *News from the States: State Legislatures Address Use of RFID Technology*, http://www.ncsl.org/programs/lis/CIP/CIPCOMM/summer04.htm#RFID.

[103] *See* Claire Swedberg, *New Mexico Kills RFID Privacy Bill*, RFID J., Mar. 16, 2005, http://www.rfidjournal.com/article/view/1449/1/1/; *see also* Kristen Power, *GMA Comments in Opposition to New Mexico RFID Bill*, http://www.gmabrands.com/publicpolicy/docs/comment.cfm?DocID=1445.

[104] H.R. 215, 47th Leg., 1st Reg. Sess. (N.M. 2005).

[105] Steve Terrell, *"Spy Chips" Legislation Clears Its First Hurdle*, SANTA FE NEW MEXICAN, Feb. 2, 2005, at A-7.

[106] Steve Terrell, *Industry Sways House Panel to Kill "Spy Chip" Regulation*, SANTA FE NEW MEXICAN, Feb. 12, 2005, at A-1.

resentatives fiercely argued to New Mexico's legislature that those guidelines should not become law.[107]

2. Privacy Advocates' Recommended Approach

Though privacy advocates perceive themselves as opposing industry lobbyists in the RFID debate, many share industry's preference for discussing solutions to RFID in national, technology-neutral terms. The position statement issued in November 2003 by thirty-five of the nation's most prominent consumer privacy and civil liberties organizations outlined a framework of rights and responsibilities applicable to RFID. It was national in scope, likely in recognition of the fact that retailers operate across state lines and of the desire to provide broad coverage against the privacy threats posed by RFID.

The position statement called for the rollout of RFID to be guided by technology-neutral Fair Information Practices (FIPs). FIPs refer to rights and responsibilities developed by a Department of Health Advisory Committee in the early 1970s and expanded upon by the Organization for Economic Cooperation and Development (OECD).[108] They apply to the collection and usage of personal information and ensure that personal information is not used in ways inconsistent with the purpose for which it was collected. The statement's authors imagined that FIPs would translate into commitments by RFID users to (1) transparency: RFID users making public their policies and practices involving the use of RFID; (2) purpose specification: RFID users giving notice of the purposes for which RFID is being utilized; (3) collection limitation: RFID users limiting collection of information "to that which is necessary for the purpose at hand"; (4) accountability: RFID users being held legally responsible for complying with these principles; and (5) security safeguards: RFID users ensuring security and integrity in transmission, databases, and system access.[109] The position statement then deemed certain RFID practices flatly incompatible with FIPs. These included prohibiting individuals from detecting RFID technology and disabling tags, coercing customers into accepting live or dormant RFID tags in the products they buy, and tracking individuals' locations absent their informed and written consent.[110]

The position statement did not provide details about the mechanism, self-regulation or legislation, through which the FIPs should be enforced. Nor did it elaborate upon the vague wording which underlay its boundaries for RFID implementation by clarifying, for example, whether purpose specification entails informing consumers about all the subsequent

---

[107] *Id.*
[108] CASPIAN et al., *supra* note 21.
[109] *Id.*
[110] *Id.*

uses of their information that might result from their purchase of products with RFID tags. Instead, it delayed the need for such resolutions, calling for a voluntary moratorium on item-level RFID tagging of consumer goods until a formal technology assessment process involving all stakeholders, including consumers, could take place.[111] The goal of the assessment is to provide a foundation for making concrete policy decisions about RFID and although not stated, the assessment is intended to stall the implementation of RFID.

In the 2004 congressional hearings, two of the privacy groups that signed the position statement—the ACLU and the CDT—elaborated upon their recommendations and specifically called for national "technology-neutral, baseline privacy legislation" based on FIPs.[112] Their willingness to employ legislation as a privacy enforcement mechanism distinguished them from the industry advocates who also testified, but the emphasis on non-RFID-specific solutions was similar. As Barry Steinhardt of the ACLU said: "I agree with industry that they need one set of standards that may apply differently in different circumstances and may reach different results in different circumstances . . . I do agree with the one set of standards, but they need to be in laws."[113] Industry's motivation in discussing RFID in technology-neutral terms was to draw scrutiny away from the technology and buy time to implement it; privacy advocates' motivation was to draw attention toward the bigger problem of the United States' emergence as a surveillance society.[114] Both the ACLU and CDT viewed RFID as raising novel privacy issues relative to other technologies, but Steinhardt urged Congress "to view them in the larger context—a world that is increasingly becoming a sea of data and databases, where the government and private sector corporations alike are gathering more and more details about our everyday existence."[115] According to his thinking:

> It will always be important to understand and publicly debate every new technology and every new technique for spying on people. But unless each new development is also understood as just one piece of the larger surveillance mosaic that is rapidly being constructed around us, Americans are not likely to get excited about a given incremental loss of privacy.[116]

---

[111] *Id.*

[112] *RFID Technology*, *supra* note 4, at 26 (statement of Paula J. Bruening, Staff Council, Center for Democracy and Technology).

[113] *RFID Technology*, *supra* note 4, at 58 (statement of Barry Steinhardt, Director of the ACLU's Technology and Liberty Project).

[114] *Id.*

[115] *Id.* at 36.

[116] *Id.*

Comprehensive privacy legislation has emerged as privacy advocates' chosen strategy because it appears to counter the surveillance trend by encouraging a culture of privacy. The benefit of baseline privacy legislation is that it not only addresses privacy with respect to RFID but it also binds the implementation of emerging technologies in ways that respect privacy. CDT Counsel Paula Bruening explained her rationale when she said:

> Every time there's a new emerging technology that involves data collection, we find ourselves back in these hearing rooms talking about how to specifically address privacy and that specific technology. Our belief is that if we have legislation that addresses collection of information no matter what the technology, we will be way ahead of the curve when it comes to the next technology that emerges. Businesses will have a better sense of what the responsibilities are in terms of putting [in] privacy-implementing policies that are privacy respectful and consumers will have a better sense of what they can expect in terms of their rights and responsibilities and their own information.[117]

Baseline privacy legislation also recognizes, in a way that the United States' sectoral approach to privacy legislation has not, that data once-gathered becomes a commodity independent of the industry that collected it. Privacy advocates gravitate toward FIPs as the underpinnings of their proposed legislation because they are well-established. Congress has demonstrated its willingness to adopt FIPs in other contexts, as with the Privacy Act of 1974 that gives citizens rights regarding the collection and use of their information by federal agencies.[118]

For privacy advocates like the CDT, the corollary to the notion that technology-neutral privacy legislation would be beneficial is that technology-specific privacy legislation would be "undesirable."[119] Bruening says: "To enact legislation specifically for RFID would risk technology mandates that are ill-suited to the future evolution of the technology."[120] In a recent article, Bruening imagines the world in 2015 after California and Massachusetts have passed RFID privacy measures.[121] In this futuristic scenario, companies are unable to assume the costs and liability of RFID tags and seek other means of monitoring inventory. To reduce storeroom theft and obtain information for behavior-based marketing research, they deploy facial recognition cameras throughout their stores, a technology

---

[117] *Id.* at 58–59.

[118] Privacy Act of 1974, 5 U.S.C. § 552(a) (2000).

[119] *Id.* at 26 (statement of Paula J. Bruening, Staff Council, Center for Democracy and Technology).

[120] *Id.* at 29.

[121] Ari Schwartz & Paula Bruening, *Multiple Scenarios for Private-Sector Use of RFID*, *in* RFID: APPLICATIONS, SECURITY, AND PRIVACY, *supra* note 19, at 275, 277–78.

which by 2010 has developed to meet demand. Data-mining companies begin buying the proprietary databases created as a result of this practice, and, in 2015, two companies announce that they have collected images of over 150 million Americans and tied them to their purchasing habits, resulting in "unprecedented consumer concern about privacy."[122] Although Bruening does not consider her vision predictive, it reflects a concern shared by other privacy advocates that RFID-specific legislation will simply lead to that technology becoming disfavored relative to another emerging technology, whose intrusions upon consumer privacy may be similarly alarming.

A second concern is that expressed by the ACLU: a focus upon a particular technology obscures from Americans the many ways in which their privacy is at risk and fails to generate the appropriate public pressure to preserve privacy.[123] Not all privacy groups are equally antagonistic to RFID-specific legislation,[124] but the weight of the most vocal members of the privacy community, with the greatest access to policy makers, has not supported it.

The privacy community's orientation toward baseline privacy legislation and ambivalence, at best, toward RFID-specific approaches has manifested itself in a lack of support for state RFID privacy measures. The response to California Senator Barbara Bowen's 2004 bill is one example. Senate Bill 1834 would have prohibited businesses from using RFID systems to track products or people unless they met certain conditions.[125] The purpose of the bill was to address the privacy issues created by RFID by permitting stores to collect the same information they gather using barcodes, but banning the use of RFID to track customers as they shopped or after they left the store.[126] The California Senate approved the bill by a vote of twenty-two to nine, but it failed to obtain passage.[127] During hearings on the bill, privacy advocates, including the ACLU and the EFF, opted not to support it.[128] Instead, they expressed general concerns about the jeopardy in which RFID places consumer privacy and reiterated the

---

[122] *Id.* at 278.

[123] Stanley & Steinhardt, *supra* note 29, at 14.

[124] *RFID Technology*, *supra* note 4, at 44 (statement of Cedric Laurant, Policy Counsel, Electronic Privacy Information Center) (recommending "that Congress should first rule on legislation specifically targeting the use of RFID in the retail sector and require clear labeling and easy removal of item level RFID tagging . . . . Then Congress should legislate in a way that protects consumers from improper use and sharing of data in both the public and private sector by establishing a legal framework based on clear information practices.").

[125] *Hearing on S.B. 1834 Before the S. Energy, Utilities & Communications Comm.*, 2004 Leg., 2003-2004 Sess. (Cal. 2004), *available at* http://www.leginfo.ca.gov/pub/03-04/bill/sen/sb_1801-1850/sb_1834_cfa_20040426_105935_sen_comm.html.

[126] *Id.*

[127] *Radio Frequency Identification Systems: Hearing on S.B. 1834 Before the Assemb. Comm. on Business & Professions*, 2004 Leg., 2003-2004 Sess. (Cal. 2004), *available at* http://www.leginfo.ca.gov/pub/03-04/bill/sen/sb_1801-1850/sb_1834_cfa_20040619_163510_asm_comm.html.

[128] *Id.*

framework that they articulated in their November 2003 position statement as the basis for an alternative bill. Although the privacy advocates phrased their stance as being "neutral" on the bill, legislative committee reports list them as being in opposition, along with the GMA.[129] In other states, privacy advocates have similarly refrained from offering support to the sponsors of state RFID privacy measures. In New Mexico, the local chapter of the ACLU did lobby for the Radio Frequency Right to Know Bill, but in Nevada, for instance, the sponsor of an RFID privacy bill reported no assistance from privacy organizations.[130] CASPIAN has endorsed RFID-specific bills that mandate labeling but not bills that require more.[131]

II. Safeguarding the Arrow

A. Baseline Privacy Solutions

The almost inevitable result of industry and privacy advocates' agreement on national, technology-neutral approaches to RFID is that the privacy regime governing RFID's implementation will be the status quo. The privacy advocates' choice, comprehensive national privacy legislation, faces barriers to passage too arduous to overcome, leaving self-regulation as the alternative that fits the settled criteria. Baseline privacy legislation's difficulties are due both to the current political landscape and to entrenched conceptions of the government's relationship to privacy within the United States. Privacy issues are traditionally bi-partisan, involving a combination of fear of oversight and concern for individual liberties that appeals to conservatives and liberals alike. However, the current Bush administration is decidedly anti-regulatory in tone, as reflected in the FTC's decision to let RFID users regulate themselves.[132]

In addition, comprehensive privacy legislation departs too far from how the United States has historically treated privacy concerns to receive near-term traction. The United States' resistance to comprehensive legislation is evident in the contrast between the ways data protection has been treated internationally and domestically. The European Union has enacted a data protection directive that significantly restricts many data collection, processing, dissemination, and storage activities for data originating in a member state. The United States has rejected that approach,[133]

---

[129] *Id.*

[130] E-mail from Sharron Angle, Assembly Member, Nevada State Legislature, to author (Apr. 6, 2005) (on file with author).

[131] Conversation with Katherine Albrecht, Founder, CASPIAN, in Cambridge, Mass. (Apr. 22, 2005).

[132] *See supra* note 57 and accompanying text.

[133] *But cf.* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 Stan. Tech. L. Rev. 1, at ¶ 43 (2001) (writing that "the concept of Fair Information Practices, like the development of a legal right of privacy, is very much an American creation" and that "[t]hose who have favored self-regulation and

instead relying upon private, market-based initiatives driven, according to Professor Nehf, "largely by the idea that individuals can effectively value their privacy and then take steps to ensure that they receive a net benefit from the collection and sharing of their data."[134] The United States' patchwork of privacy laws results in incomplete protection of individuals' privacy, but for Professor Howard Cate, this "reflects a constitutional calculation that such harm is less threatening to the body politic than the harm associated with centralized privacy protection [and] government interference with the information flows necessary to sustain democracies and markets."[135]

The privacy laws that the United States has enacted seem aimed at restoring individuals' ability to protect their own privacy in response to particular technologies and industry practices perceived as hindering individuals' capacity to self-rely. The Fair Credit Reporting Act of 1974,[136] for example, regulates the credit reporting industry and provides consumers with a degree of agency in allowing them to request copies of their credit transaction records and dispute errors. More recently, the Children's Online Protection Act of 1998, which restricts the use of information gathered from children under age thirteen by Internet websites unless they have obtained verifiable parental consent, has been said to "facilitate—not interfere with—the development of private mechanisms and individual choice as the preferred means of valuing and protecting privacy."[137] Congress is attentive to privacy concerns; the 108th Congress saw the introduction of privacy bills dealing with identity theft, telemarketing, spyware, misuse of social security numbers, and wireless telephone spam.[138] This list reflects that those bills which targeted private actors continued to take a largely sectoral approach. As even the ACLU has acknowledged, despite its hopes, baseline privacy legislation may never become a reality.[139]

The unlikely success of baseline privacy legislation as *the* legal solution to RFID is problematic because RFID is arriving, with all its attendant capabilities for profiling, tracking, and targeted marketing, and the

---

promoted market-based solutions to the privacy problem over the last few years have tried to ignore this history.").

[134] Nehf, *supra* note 52, at 4.

[135] Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 232 (1999).

[136] 15 U.S.C. §§ 1681–1681t (2000).

[137] Cate, *supra* note 135, at 225.

[138] *See, e.g.*, Identity Theft Consumer Notification Act, H.R. 818, 108th Cong. (2003) (sponsored by Reps. Gerald Kleczka (D-Wis.) and Paul Ryan (R-Wis.)); Online Privacy Protection Act of 2003, H.R. 69, 108th Cong. (2003) (sponsored by Rep. Rodney Frelinghuysen (R-N.J.)); Telemarketing Relief Act of 2003, H.R. 526, 108th Cong. (2003) (sponsored by Reps. Nancy Johnson (R-Conn.) and Rob Simmons (R-Conn.)); Social Security Number Misuse Prevention Act, H.R. 637, 108th Cong. (2003) (sponsored by Rep. John Sweeney (R-N.Y.)); Wireless Telephone Spam Protection Act, H.R. 122, 108th Cong. (2003) (sponsored by Rep. Rush Holt (D-N.J.)).

[139] Stanley & Steinhardt, *supra* note 29.

existing market forces and self-regulations do not protect consumers. RFID currently is an expensive proposition for retailers to implement, but companies like Hewlett Packard and IBM have been investing heavily in improving the technology, pledging to spend $150 million and $250 million over the next five years respectively.[140] The price of RFID tags dropped from forty cents to a quarter over the last year, and there is no reason to believe that it, as well as the cost of the hardware and software required to support RFID systems, will not continue a steep decline. Though some commentators believe that widespread, item-level RFID tagging may be years away, RFID tags do not need to be on every cereal box or pack of gum before they are sufficiently pervasive to enable significant profiling and tracking of consumers. Wal-Mart's CIO Linda Dillman has testified before Congress that Wal-Mart expects more than 20,000 of its domestic suppliers to be participating in its RFID program by the end of 2006.[141] During that time, Wal-Mart will focus on case and pallet-level tagging, but Dillman says there will be instances where consumers will purchase products bearing an RFID tag. Given the resources that have been spent developing RFID and its many potential benefits, RFID's arrival in consumer environments appears imminent and inescapable.

Experience demonstrates that legally unenforceable self-regulation will not be a sufficient limitation on RFID's threat to privacy. Despite industry's assurances, there are countless examples of companies behaving in ways that would not serve their bottom lines if they were exposed. The companies persist nonetheless, either because the risk seems worthwhile or because they have difficulty maintaining oversight over their own operations. Profit motivation would appear to dictate that ChoicePoint, one of the world's largest and most successful data brokers, with 19 billion public and private records, would not sell personal information on 145,000 Americans to a criminal ring of ID thieves masquerading as small businesses.[142] Yet such an event occurred. ChoicePoint's Chief Executive Officer portrayed his company as exceptional for alerting the sheriff's office to the compromised information: "Most companies might not have gone to law enforcement, and this would have been buried away."[143]

---

[140] Steve Terrell, *Bills Seek to Protect Privacy*, SANTA FE NEW MEXICAN, Jan. 16, 2005, at A-9. *See also RFID Technology*, *supra* note 4, at 37 (statement of Barry Steinhardt, Director, Technology & Liberty Program, ACLU) ("If we at the ACLU have learned anything over the past decade, it is that seemingly distant privacy invasions that sound right out of science fiction often become real far faster than anyone has anticipated.").

[141] *See RFID Technology*, *supra* note 4, at 13.

[142] Tom Zeller, Jr., *Breach Points Up Flaws in Privacy Laws*, N.Y. TIMES, Feb. 24, 2005, at C-1. Also, in March 2005, Lexis Nexis announced that hackers broke into one of its databases and gained access to the personal files of perhaps 32,000 people. CBS News, *Hackers Hit Lexis Nexis Database*, http://www.cbsnews.com/stories/2005/03/10/tech/main679237.shtml (last visited Nov. 19, 2005).

[143] Zeller, *supra* note 142, at C-1.

There is little reason to expect that retailers, if left unbound by the force of law, would be immune to breaches of consumer trust.

In addition, consumers cannot, as retailers advocate, be entrusted to enforce their own privacy preferences by voting with their feet and frequenting the competition. This is especially true in the context of RFID. In order for individuals to self-police their own privacy rights effectively, they must be able to value those rights, assess their worth relative to the benefits to be achieved by sacrificing them, and protect the rights they decide to preserve by identifying and holding accountable those who violate them.[144] These prerequisites cannot be met in unconstrained RFID systems. The data collection process is totally invisible to consumers, thus depriving them of the opportunity to trade-off the disclosure and retention of their personal information. The data collection process is also ongoing; to make rational decisions consumers must value not only the information their tags are transmitting at the present moment, but at all future moments. Furthermore, consumers are not informed of how their data may be aggregated and what harms may result. Indeed, the retailer selling tagged goods to consumers might not even possess this knowledge, given the possibilities for later information sharing or capture by unauthorized third parties. The result is that consumers cannot accurately determine how much it matters to them to keep their information private. The opaqueness of RFID systems means too that it is difficult for consumers to tell when their privacy has been violated and by whom, making it a challenge to penalize the perpetrators.

The conditions of market failure are compounded by the fact that consumers fundamentally do not understand how RFID technology works. An October 2003 survey by the consulting firm Capgemini revealed that despite all the debate surrounding RFID, only a quarter of respondents had any idea what the technology was.[145] This was true even though a considerable number of respondents routinely used the EZ-Pass toll payment system enabled by RFID. In another study, a group of librarians, chosen for their technology focus, were tested on their knowledge of RFID. They scored no better than they would have if they had randomly guessed at the answers. The authors of the study concluded that they did not have a substantive grasp of RFID technology.[146] A lack of technical knowledge

---

[144] Nehf, *supra* note 52, at 18–28.

[145] Transcript of Fed. Trade Comm'n Workshop on Radio Frequency Identification at 131–33 (2004), *available at* http://www.ftc.gov/bcp/workshops/rfid/transcript.pdf (remarks by John Parkinson, Vice President and Chief Technologist, Capgemini). Awareness of RFID seems to be increasing, though it still hovers below fifty percent. In a RFID Consumer Buzz survey conducted by Columbus, Ohio-based market intelligence company Bigresearch in March 2005, forty-one percent of 8500 adults said they had heard of RFID. That figure is up from twenty-eight percent when the same survey was conducted in September 2004. Jonathan Collins, *Consumers More RFID-Aware, Still Wary*, RFID J., Apr. 8, 2005, http://www.rfidjournal.com/article/articleview/1491/1/130.

[146] Lee S. Strickland & Laura E. Hunt, *Technology, Security & Individual Privacy: New*

about RFID could explain why consumers who are highly concerned about their own privacy, as many consumers profess to be,[147] might nevertheless fail to protect it if opportunities existed to do so. They would simply not be aware of which actions to take. Self-regulation may help rectify the situation by, for example, encouraging consumer education notices to be placed on all RFID-tagged products. However, unless it consistently makes the data gathering and usage process visible and comprehensible to consumers, a self-regulatory regime will operate sub-optimally.

If today's background legal regime offers consumers little privacy protection against RFID, if comprehensive privacy legislation is unrealistic, and if self-regulation is inadequate, then an alternative legislative solution might be required.[148] Industry advocates are correct that legislation will burden the implementation of RFID technology, but a lack of legislation early in the deployment process may entail costs as well. It can be more efficient to incorporate privacy protections into a technology's design and installation than to attempt to build privacy into already established systems in response to controversy resulting from privacy violations. It is not even necessary for such back-tracking to occur for the status quo to seem expensive in retrospect. Professor Minow argues that what people experience, they come to expect. A failure to attend to privacy concerns results in a downward spiral that reduces "both the scope of experiential privacy and people's hope of privacy."[149] This is actually what retailers are hoping will happen as they attempt to forestall legislation; people will become accustomed to RFID and less alarmed by its profiling and tracking capabilities. Minow warns, however, that "before we know it, such a downward spiral could affect the very sense of self people have—the sense of room for self-expression and experimentation, the sense of dignity and composure, the sense of ease and relief from public presentation."[150] Though the value of privacy is difficult to quantify relative to supply chain outlays, to the extent that people strongly cherish privacy, they should be willing to sacrifice some degree of technological progress to secure it.[151]

Unfortunately, the agreement between industry advocates and privacy advocates on national, technology-neutral approaches has not encouraged

---

Tools, New Threats & New Public Perceptions, 56 J. AM. SOC'Y INFO. SCI. & TECH. 221, 232 (2005).

[147] Proprietary surveys conducted by Columbia Law Professor Alan Westin through his Privacy and American Business information reporting service suggest that privacy concerns have been rising over time. Self-professed "privacy fundamentalists" stand at thirty-seven percent of the U.S. population. Perrin, *supra* note 49, at 62 n.9.

[148] *But cf.* Paul M. Schwartz, *Beyond Lessig's Code For Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 783 (writing that "the most powerful limits on access to personal information are not always the best for society as a whole").

[149] Galison & Minow, *supra* note 50, at 259.

[150] *Id.*

[151] Campbell, *supra* note 67, at 102.

the investigation of innovative alternative solutions to RFID's privacy threats. If both sides of the privacy debate concur that RFID is not "the issue," then it drops off the priority list for policymakers. Representative Darrell Issa (R-Cal.) demonstrated this likelihood at the conclusion of the July 2004 congressional hearings on RFID when he said: "[I]sn't this really more a matter of us legislating what you do with the information, how long you can keep it and what is appropriate, rather than the question of whether or not you can initially collect it?"[152] The way in which privacy advocates have discussed technology-neutral legislation as desirable and technology-specific legislation as undesirable encourages the either/or mentality reflected in Representative Issa's statement. Those who favor baseline privacy solutions have made their choice and need not explore further.

This message is troubling, and not simply because baseline privacy legislation is politically unrealistic. Even if baseline legislation achieved passage, it is not a sufficient solution to the privacy challenges posed by RFID because it does not adequately target data collection as opposed to data use. Baseline privacy legislation offers many benefits, but by its nature, which is technology-neutral, it tends to focus more on how data will be managed than how it is gathered, a technology-dependent process.

This bias is evident in the five principles posited by the FIPs that privacy advocates would like to underlie comprehensive privacy legislation: (1) There must be no personal-data record keeping systems whose very existence is secret; (2) There must be a way for an individual to find out what information about her is in a record and how it is used; (3) There must be a way for an individual to prevent information about her obtained for one purpose from being used or made available for other purposes without her consent; (4) There must be a way for an individual to correct or amend a record of identifiable information about her; (5) Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data and take reasonable precautions to prevent its misuse. None of these principles addresses the extent to which personal information should be gathered. In their November 2003 position statement, privacy advocates gave their express approval to the OECD's iteration on FIPs. The OECD's formulation does add a collection limitation principle, but it states only vaguely that limits should exist and that any personal information ought to be gathered lawfully and, where appropriate, with the consent of the subject.[153] As applied by privacy advocates to RFID, collection limitation translates into instructions highly subject to co-option by RFID users: "The collection of in-

---

[152] *RFID Technology, supra* note 4, at 57.

[153] Org. for Econ. Co-operation and Dev., Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), *available at* http://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html.

formation should be limited to that which is necessary for the purpose at hand."[154] Such a standard would even make it difficult for consumers and law enforcement officials to determine when violations of privacy rights occurred, since the "purpose" of information collection may be ever evolving. FIPs neglect the reality that preserving the confidentiality of personal information becomes a simpler affair if that information is not collected at all.

FIPs seem aimed at systems not entirely applicable to RFID: ones with clearly identifiable data collectors whom consumers deliberately entrust with their information to facilitate a transaction. The aim then becomes making sure the data collectors are subject to meaningful restraints on using and sharing that information.[155] RFID systems complicate this framework because they allow anyone with a reader to become an undetectable data collector. FIP principles, such as a consumer's right to access and amend her personal records, have no force in this context. If the consumer is not aware that her data is being gathered, she will have no way of recognizing the need to contact someone about the accuracy of her records or of determining the identity of the data collector. Once her information becomes digitalized, it can be bought and sold instantaneously; information obtained from unauthorized scanning can thereby achieve a wide audience without its source becoming traceable.

Even when there is a clearly identifiable data collector, such as a retailer who informs consumers about its RFID practices, FIPs regulate personal information at its most vulnerable state. FIPs can threaten damages for data collectors who do not handle data as prescribed, but, except in rare instances, consumers may never learn of privacy violations. It is difficult for consumers and law enforcement officials to maintain control over the use of digitalized information, and the task of auditing the amounts of data collected through RFID systems would be immense. Much of the power of RFID is in information systems. While baseline privacy legislation offers consumers some protection, it is not complete in the context of RFID.

B. Technology-Specific Privacy Legislation

The gaps in consumer protection left by baseline privacy legislation suggest the desirability of another model: technology-specific legislation. Technology-specific legislation allows for collection limitation provisions particular to RFID, which makes it more rigid than baseline privacy legislation but also more nuanced. Technology-specific legislation seems appropriate to systems like RFID in cases where (1) consumers do not understand how a technology works upon them; (2) baseline provisions

---

[154] *Position Statement*, *supra* note 21.
[155] Weinberg, *supra* note 36, at 95.

do not meaningfully proscribe information collection; and (3) baseline provisions are often unenforceable after instances of information misusage.[156] Technology-specific legislation is worth considering when any one of those three factors is present, but when all three factors are realized, as they are with RFID, it has clear utility.

The lack of attention privacy advocates have given technology-specific RFID legislation means that they need to engage in significant dialogue with industry representatives, consumers, and government officials before shaping its terms. One could imagine that legislation might require RFID users to notify individuals of the technology's presence through clear and conspicuous product labels and readers that emit a tone or a light when extracting information. The legislation could also mandate that all RFID tags be easily disposable by consumers.[157] The maker of Pantene shampoo has experimented with hiding RFID tags in a part of its flip-top containers that requires a screwdriver to access; this should be prohibited.[158]

A significant benefit of RFID-specific legislation would be its consumer education effects. Privacy advocates have been rallying against RFID for years but have not managed to alert the majority of consumers to its existence. The same Capgemini survey that revealed that most consumers have never heard of RFID, however, also showed that when they learned about it, they were troubled. Almost seventy percent of respondents said they were "extremely concerned" about the possibility of third parties using their data; sixty-seven percent were concerned they would be targeted with direct marketing; and sixty-five percent were concerned consumers would be tracked through their purchases.[159] The stealth nature of RFID means that it takes more than a consumer education campaign to allow consumers to recognize the technology and when it is in use; it takes direct warnings like labels that include information on what RFID systems are, where they are operating, how they collect data, what risks they pose to privacy, and how they may be disabled. While privacy advocates worry that technology-specific legislation will give consumers the sense that they can preserve their information privacy more than is actually possible, there is also the chance that technology-specific legislation will force consumers to confront a heretofore hidden element of surveillance infrastructure and stimulate curiosity about surveillance systems at large.

---

[156] Another appropriate target of technology-specific laws may be video surveillance cameras, which could be subject to restrictions governing their use and how long their images are stored.

[157] *See* ELEC. PRIVACY INFO. CTR., GUIDELINES ON COMMERCIAL USE OF RFID TECHNOLOGY (July 9, 2004), http://www.epic.org/privacy/rfid/rfid_gdlnes-070904.pdf.

[158] Transcript of Federal Trade Commission Workshop on Radio Frequency Identification at 234 (2004), *available at* http://www.ftc.gov/bcp/workshops/rfid/transcript.pdf (remarks by Katherine Albrecht, Director, CASPIAN).

[159] Katherine Albrecht & Liz McIntyre, *RFID: The Big Brother Bar Code*, 6 AM. LEGIS. EXCHANGE COUNCIL POL'Y F. 49, 53 (2004).

Another advantage of technology-specific legislation is that it is tailored. FIPs provide for notice that does not automatically translate into informed decision-making on RFID issues for consumers. Wal-Mart currently discloses the presence of RFID tags in its stores through a "shelf-talker."[160] This tear-off leaflet contains as much public relations jargon as it does useful information, touting RFID for allowing improved product visibility and assuring consumers that it is simply the next generation of bar codes.[161] The leaflet tells consumers that some products have RFID tags, but does not state which products. Consumers are instructed to look for a symbol, a cube containing the letters EPC, on a product's outer packaging. The leaflet concludes that consumers may keep their RFID tags or discard them, but it does not reveal how to recognize the miniscule tags. Meaningful consumer choice does not exist if the procedures required to exercise it are so burdensome to investigate and implement. Technology-specific legislation can improve the efficacy of RFID notices by deliberately guiding their scope, content, and placement.

The practical result of RFID-specific legislation would be that consumers would be cued when retailers engage in data-gathering through RFID and have means of hindering the fine-grained collection of their personal information. There is the chance that once legislation confronts consumers with RFID use, a popular movement will arise to keep RFID technology in warehouses and backrooms and off store floors. In 2003, CASPIAN's threatened consumer boycott of Benetton proved enough to compel the retailer to retract its plans to embed RFID tags into its entire Sisley line of clothing.[162] Even if enough consumers prove willing to tolerate RFID on store floors, however, those consumers who are privacy sensitive could take actions to prevent their purchases from being linked to their name by paying in cash. This alone would not eliminate the ability of readers to scan their possessions, but it would impede data-gatherers' ability to link those possessions to consumers' personally identifying information. Consumers would then have the option to remove their tags, which would end the possibility of scanning once they left the store.[163] If RFID-specific legislation required tags to be incorporated into products' disposable packaging, tag removal would require no more effort from consumers than they already expend.

Violations of RFID-specific legislation would be recognizable and enforceable. Consumers would not have to wait years for courts or agencies to decide how a broad collection limitation principle applied to RFID. Nor

---

[160] *See* STAFF OF THE FED. TRADE COMM'N, *supra* note 3, at 43 (2005) (containing photocopy of Wal-Mart's "shelf-talker").

[161] *Id.*

[162] Press Release, Katherine Albrecht, CASPIAN, No RFID Tracking Chips in Clothing! (Apr. 9, 2003), *available at* http://www.boycottbenetton.com/PR_030407.html.

[163] *See* Weinberg, *supra* note 36, at 96–97 (describing benefits of disposable tags). *Cf. Position Statement*, *supra* note 21 (expressing concerns about in-store tracking).

would they have to attempt to remedy violations ex post facto, after their information has been irretrievably transmitted. Rather, law enforcement officials and regulatory inspectors could be proactive on behalf of consumers, using readers to scan store floors for RFID tags and ensuring the implementation of legislated procedures governing data collection.

The goal of technology-specific legislation is fundamentally true to the notion underlying much of United States privacy legislation, which is to enhance consumers' ability to recognize privacy invasions and prevent undesirable ones from recurring. This posture is also arguably one of its greatest drawbacks. According to Professor Nehf, it is a myth that technology-specific legislation will allow consumers to navigate RFID systems in ways that suit their varying sensitivities. Notice and choice do not lead to effective consumer privacy unless those mechanisms enable consumers to value the information they are disclosing as it may be used not just by the retailer, but also by every affiliate, interested third party, or identity thief who may subsequently obtain and aggregate it. Studies show that consumers will dispose of their information relatively cheaply when they do not have a full sense of what is going to happen to it.[164] The worry is that retailers will find a way to induce even consumers who are concerned about their privacy to refrain from policing the collection of their data and the existence of some RFID-specific legislation will be used to silence calls for further reform. For those fearful that the good of technology-specific legislation will become the enemy of perfect privacy protection, that any legislation which allows RFID tags onto store floors expresses inappropriate tolerance for the privacy invasions they entail, that legislation will lull consumers into passivity over RFID because uncritical belief in choice mechanisms is the American Way though privacy is not in fact safeguarded, the answer is that against a legal background of no consumer protection, the feasible policy choices are not complete and incomplete privacy protection, but something and nothing. Furthermore, technology-specific legislation contributes to reduced data gathering. The advantages of technology-specific legislation accrue primarily to informed consumers, but the consumer education aspects of the legislation simultaneously help to increase their number.

Other drawbacks of RFID-specific legislation should be acknowledged, though they are not as great as either retailers or privacy advocates make them seem. Some additional critiques of RFID-specific legislation do not address whether technology-specific legislation is worthwhile, but whether it is sufficient. The argument that RFID-specific legislation does not guide emerging technologies is of that variety, as is the assertion that the means of data-gathering become irrelevant to privacy protection once that data has been compiled and commodified. These are reasons why privacy advo-

---

[164] *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1503–04 (2000); *see also* Nehf, *supra* note 52, at 22.

cates should continue lobbying for baseline privacy legislation, but they are not rationales for shunning RFID-specific legislation altogether.

Another concern is that RFID-specific legislation will not be resistant to time. Simson Garfinkel, author of the *RFID Bill of Rights*, expresses this worry when he writes: "Legislation . . . is a slow process, often at pains to keep pace with rapid technological advance . . . . Technologies, after all, change faster than laws can."[165] His fear that RFID-specific legislation may become obsolete immediately after it is passed may be assuaged by past examples of the United States deliberately and successfully regulating high-tech monitoring systems. Congress has enacted privacy laws for telephone networks, computer databases, videotape rentals, automated health records, electronic mail, and polygraphs that retain force today.[166] These technologies have represented enough of an advance that there have been no immediate substitutes. More importantly, drafters of high-tech legislation have remained focused on achieving their policy aims by eliminating behavioral abuses of technologies as opposed to making detailed technological prescriptions. It has not been their intent to prohibit new technology, but rather to establish public trust in its usage. RFID could expect similar treatment, and retailers would remain free to innovate within the established guidelines.[167]

Of course, like baseline privacy legislation, RFID-specific legislation cannot offer meaningful consumer protection unless it is enacted. On the federal level, there are some indicators that its chance of passage compares favorably to baseline legislation. Its limited scope accords with the United States' distaste for omnibus privacy legislation, and its likely provisions fit the traditionally accepted aim of enhancing consumers' ability to protect themselves against distinct privacy abuses. Technology-specific legislation also benefits, relative to baseline legislation, from the utilitarian calculus used by lawmakers to weigh the costs and benefits of new privacy legislation. This computation disadvantages privacy legislation as a whole because the costs of privacy invasions, compared to businesses' costs in administering a new piece of legislation, are difficult to quantify. The expenses associated with RFID-specific legislation are easier to measure, however, than those associated with sweeping privacy reform.

Finally, RFID-specific legislation can be analogized to the spyware legislation that has received attention in Congress. In the 108th Congress, the House passed two bills addressing the privacy aspects of spyware and the Senate Commerce Committee reported one.[168] Debate resumed in the

---

[165] Simson Garfinkel, *An RFID Bill of Rights*, TECH. REV., Oct. 2002, at 35, 35, *available at* http://www.simson.net/clips/2002/2002.TR.10.RFID_Bill_Of_Rights.pdf.

[166] This list can be found in Rotenberg, *supra* note 133, at ¶ 26.

[167] Weinberg, *supra* note 36, at 97 (suggesting retailers might incorporate more information permanently into consumer goods through a non-wireless bar code, enabling paperless returns without forcing consumers to keep RFID tags active post sale).

[168] H.R. 2929, 108th Cong. (2004); H.R. 4661, 108th Cong. (2004); S. 2145, 108th Cong.

109th Congress. Spyware does not have a precise definition, but it refers to software downloaded over the Internet onto individuals' computers without their knowledge.[169] Spyware enables the monitoring of computer users' activities, the recording of their key strokes, and the relaying of the personally identifiable information thereby captured to unauthorized recipients over the web. RFID resembles spyware in that it is an "Internet of things,"[170] allowing objects to talk to readers much in the way computers speak with each other. To the extent Congress has proved amenable to spyware legislation, it may consider RFID legislation as well. Still, despite these indicators, a safe conclusion is that, while RFID-specific legislation would fare better in Congress than baseline privacy legislation, its odds of passage are poor. The reality is that there are no RFID privacy bills pending before Congress and the Republican Senators on the High Tech Task Force have committed themselves to protecting RFID from regulation, making national RFID-legislation impossible in the near term.[171]

Where RFID-specific legislation does have a chance of enactment is at the state level. Nine state RFID consumer privacy bills were introduced in 2005, following five such state bills the previous year.[172] Several of the 2005 bills were more ambitious than the 2004 predecessors, suggesting that as legislators have learned more about RFID, they have become more concerned with its dangers.[173] Maryland's and Virginia's 2005 bills provided for commissions that would study RFID in greater depth and make recommendations for future legislation. New Hampshire, Missouri, Nevada, and Tennessee introduced legislation that would mandate appropriate labels on all products containing RFID tags. The Massachusetts, New Mexico, and South Dakota bills added a combination of tag disposal requirements and data use restrictions.[174] These bills had bipartisan backing, having been introduced by a mix of Republican and Democrat legislators.

(2004).

[169] MARCIA S. SMITH, CONG. RESEARCH SERV., *SPYWARE: BACKGROUND AND POLICY ISSUES FOR CONGRESS*, CONGRESSIONAL RESEARCH SERVICE 1 (2005).

[170] *See, e.g.*, *RFID and the Internet of Things*, DIGITAL ID WORLD, Nov.-Dec. 2003, at 66, 67, *available at* http://magazine.digitalidworld.com/Nov03/Page66.pdf.

[171] Press Release, *supra* note 101.

[172] *See* 2005 bills cited *supra* note 27: Maryland (H.B. 354), Massachusetts (H.B. 1447, S.B. 181), Missouri (S.B. 128), Nevada (A.B. 264), New Hampshire (H.B. 203), New Mexico (H.B. 215), South Dakota (H.B. 1136, H.B. 1114), Tennessee (H.B. 300, S.B. 699), and Virginia (H.B. 1304); 2004 bills: California (S.B. 1834), Maryland (H.B. 32), Missouri (H.B. 867), Utah (S.J. Res. 10), and Virginia (H.B. 1304).

[173] Ronald E. Quirk, Jr., *Don't Get Behind the Regulatory Eight Ball*, RFID J., Apr. 11, 2005, http://www.rfidjournal.com/article/articleview/1484/1/133/. Many state lawmakers who sponsored RFID privacy bills stated that the Wal-Mart and Target mandates prompted their decision to push for those laws.

[174] For example, South Dakota H.B. 1136 would require (a) a retailer using an EPC RFID system to obtain written consent from a consumer before collecting personally identifiable information from that consumer by means of an RFID system or before disseminating that information; (b) the consumer to have access to his/her data; (c) a retailer who collects individual data via RFID to secure that data through reasonable measures; and (d) a retailer to detach or destroy all RFID tags before the consumer leaves the store. *See id*.

They also received widespread support, for example, passing committee, House, and Senate votes by large margins in New Mexico, Utah, and California, respectively, though ultimately failing to obtain passage.

States are well suited for the role of privacy pioneer; they have traditionally served as laboratories for privacy initiatives later adopted at the federal level. In one recent year, states introduced 2367 privacy bills and enacted 786 into law.[175] The states where RFID-specific legislation is pending, especially Massachusetts and New Hampshire, have strong track records of enacting legislation in defense of privacy.[176] The reason that no state-level RFID-specific bill has yet been successful is that, as in New Mexico, industry lobbyists have passionately committed themselves to defeating the bills. This admittedly makes their passage difficult. Nevertheless, an intensive pro-legislation campaign organized by the privacy community may be enough to counteract industry's efforts; the outcome is not apparent because privacy advocates have thus far failed to offer the bills their total support. If privacy advocates truly want protections for consumers against RFID, they will work with legislators to shape the provisions and secure the passage of RFID-specific state bills.

The attitude on all sides of the privacy debate has been that the result of state legislation for RFID-tagged goods would be a hodgepodge of differing requirements confusing to retailers and consumers alike. This analysis fails to account for how state legislation can lead to protection that transcends state boundaries through a leveling-up process. First, some provisions of an RFID-specific law, such as those requiring notice of RFID to be directly on product packaging, would inevitably require compliance by the manufacturer as well as the retailer. Once some states require labels, manufacturers seeking the efficiency of uniform processes may find it less costly to label all RFID-tagged products regardless of their destination than to discriminate amongst products based on their intended point-of-sale. A similar calculation may lead to disposable tags becoming the norm for all products, even when they are not mandated everywhere. Such an outcome would expand consumer education and choice benefits from states that have enacted RFID laws to ones that have refrained.

Second, retailers would likely respond to state RFID laws by calling for federal legislation. The Progressive Policy Institute has explicitly advised Congress to monitor state legislative activities with an eye toward preempting restrictive and conflicting state legislation. Once preemption is under congressional consideration, though at the instigation of industry representatives, the subsequent debate need not mean doom for privacy-

---

[175] These numbers are from 1998. Privacy and American Business Information Reporting Service, *Privacy Legislation in the States*, http://www.pandab.org/v5n3priv.html.

[176] Rodger Doyle, *Thwarting Big Brother: The Job of Blocking Prying Eyes Falls Mostly to the States*, SCI. AM., Dec. 2004, at 33, 33 (classifying states on the basis of their track record in defense of privacy). Massachusetts is one of the most privacy-friendly states in the nation. *Id.*

enhancing, RFID-specific legislation. Rather, the national discussion could lead to a greater awareness of RFID privacy threats, making a complete override of privacy protections politically unpopular among both Republican and Democrat constituents, who currently lack knowledge about RFID. The result would be a compromise between industry representatives and privacy advocates that allows for the enactment of measures that, while not as sweeping as those proposed in every state, nonetheless provide meaningful protection for consumers.

There is precedent for state regulation leading to expansions of privacy protection nationwide. One example stemmed from the launch of caller ID, which in the 1980s represented, in the words of privacy advocate Marc Rotenberg, "a radical change, from a privacy viewpoint, in the architecture of the nation's telephone system."[177] Caller ID transferred from telephone callers to telephone companies the right to determine when their identity or location would be disclosed to others.[178] A woman phoning her children from a battered woman's shelter, for example, became compelled to reveal her whereabouts to her spouse.[179] State regulatory bodies uncomfortable with caller ID adopted strong privacy measures, which took the form of technical rules that allowed customers to regain control over the disclosure of their personal information.[180] Some states permitted callers to dial *67 and block calls on a per-call basis; others added blocking on a per-line basis. When the telephone companies finally crystallized the technical standards for caller ID nationwide, they incorporated the public's interest in protecting privacy.[181] The FTC eventually intervened to regulate caller ID and it mandated per-call, though not per-line, blocking options on interstate calls.[182] The result was still an increase in consumer privacy protections relative to what market forces and self-regulation might have afforded.[183]

More recently, ChoicePoint's sale of consumers' personal data to ID thieves was exposed due to California's security breach notification law, the only such law in the nation. After ChoicePoint learned its systems had been compromised, it first contacted just the 35,000 Californians affected because they were the only people it had a legal obligation to inform. Word of the breach emerged from California, however, pressuring ChoicePoint to voluntarily notify the other 110,000 consumers harmed around the nation.[184] Notification might have proceeded with more haste

---

[177] Rotenberg, *supra* note 133, at ¶ 12.
[178] *Id.*
[179] *Id.* at ¶ 13.
[180] *Id.* at ¶ 14.
[181] *Id.*
[182] FCC Calling Party Telephone Number Privacy Rule, 47 C.F.R. § 64.1601 (2005); FCC Finalizes Rules for Caller ID, Report No. DC 95-71 (May 5, 1995), *available at* http://www.fcc.gov/Bureaus/Common_Carrier/News_Releases/1995/nrcc5049.txt.
[183] *Id.* at ¶ 12.
[184] Zeller, *supra* note 142, at C-1.

had there been national, comprehensive privacy legislation overseeing the handling of all personal data. Yet, in the absence of such a law, California's statute provided consumers across the country with a measure of protection that would have otherwise been lacking. State RFID-specific legislation similarly has the potential to safeguard consumers nationwide.

Conclusion: Mission Impossible

"We know our privacy is under attack," Simson Garfinkel wrote in his book *Database Nation*. "The problem is that we don't know how to fight back."[185] This Note is meant to inspire privacy advocates to rethink the near-exclusive focus on national, baseline privacy legislation they share with industry representatives and to work with state legislators in crafting and lobbying for RFID-specific privacy measures that establish barriers to data collection in addition to simply data misuse.

Privacy advocates who are convinced by this Note's argument may find it difficult not to experience moments of self-doubt as they contemplate RFID labels and removable tags. They may feel similarly to the science fiction writer David Brin: "It is already far too late . . . . The *djinn* cannot be crammed back into its bottle. No matter how many laws are passed, it will prove quite impossible to legislate away the new surveillance tools and databases. They are here to stay. Light *is* going to shine into nearly every corner of our lives."[186] Brin is not sanguine about RFID-tagging; he believes that "RFID chips will be incorporated into most products and packaging . . . . [T]racking on vast scales, national and worldwide, will emerge in rapid order."[187] His counter-intuitive response is a "transparent society" that freely permits RFID collection efforts. A transparent society is categorized by constant and pervasive surveillance; the innovation is that the general public obtains access to the vast quantities of personal information now gathered into databases by commercial entities.[188] Surveillance becomes an equal opportunity proposition; Wal-Mart can collect extensive amounts of data about its customers through RFID systems, but the company's top 100 executives must post exactly the same type of information about themselves and their families in open databases.

---

[185] Simson Garfinkel, Database Nation 5 (2000).

[186] David Brin, The Transparent Society: Will Technology Force us To Choose Between Privacy and Freedom? 8–9 (1998). Sun Microsystems, Inc. CEO Scott McNealy also famously suggested that the battle for privacy was lost before it began with his statement: "You have zero privacy. Get over it." The comment responded to a question at a product launch. Edward C. Baig et al., *Privacy: The Internet Wants Your Personal Info. What's in It for You?*, Bus. Wk., Apr. 5, 1999, at 84.

[187] David Brin, *Three Cheers for the Surveillance Society*, Salon.com, Aug. 3, 2004, http://www.salon.com/tech/feature/2004/08/04/mortal_gods/.

[188] *See also* Garfinkel, *supra* note 185, at 13–15, 35 (arguing that a national databank run by the government might protect privacy better than a society without regulation of personal information).

Brin's rationale for his radical proposal is that the future is a stark choice: a surveillance society in which there is an imbalance of power between the collectors of information and those who are subject to collection, or a surveillance society in which the potential for abuse and discrimination is eliminated by the fact that everyone's actions are viewable. He addresses the fear that people will obsessively watch over others if given the opportunity by assuring, "in a society of full disclosure, people will learn to ignore the vast amount of personal information made available and find better uses for their time than spying on their peers. Since everyone has something to hide, no one will look for the flaws of others."[189] The values privileged in Brin's transparent society are equality and accountability. Wal-Mart and consumers are on even ground, in that both can access and use the same personal information. Because all actions are monitored, consumers can protect themselves from the effects of information misuse by holding anyone responsible, be they a corporation or a third party, who acts with malicious intent. Brin compares his approach to the strategy of reciprocal deterrence that existed during the Cold War arms races: when everyone has information about others, everyone will be equally vulnerable and a balance of power will emerge inhibiting detrimental uses of personal data.[190] Brin's idea was initially received as a science fiction concept, but it has gained credibility as the best available option in a world populated by RFID tags and other surveillance devices. Its appeal is seductive: it promises to allow society to enjoy the benefits of developing technologies while mitigating possible abuses stemming from information collection and analysis.

Brin's vision—and its corresponding defeatism about privacy-enhancing legislation—is not one to which privacy advocates should succumb. This Note has emphasized responses to RFID-tagging that are politically feasible. It would be close to impossible, even in the aftermath of major privacy scandals, to convince legislators and the public in general to accept the trade-offs inherent in constant monitoring.[191] Brin claims that transparency is not about eliminating privacy to secure equality and accountability; it is about spreading the power to hold responsible those who violate it. His definition of privacy implies "serenity at home and the right to be let alone."[192] His conception of privacy protection focuses on eliminating the

---

[189] Tal Z. Zarsky, *Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society*, 58 U. MIAMI L. REV. 991, 997 (2004) (summarizing the ideas of David Brin) (footnote omitted).

[190] BRIN, *supra* note 186, at 254.

[191] Professor Jessica Litman describes Brin's proposal as even less plausible than data privacy solutions that have already failed adoption, leading her to ask whether we "have a wrong with no credible remedy." Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1303 (2000). The answer, as discussed *infra*, is that we have a wrong with no one remedy.

[192] BRIN *supra* note 186, at 334 (referencing Samuel Warren & Louis Brandeis, *The Right*

harms that might result from the abuse of collected data. It fatally neglects that in the eyes of many the sheer act of collecting information constitutes harm in itself.[193] Constant surveillance "inhibits daily activities, promotes conformity, causes embarrassment, and interferes with the creation of intimacy."[194] Preserving unmonitored choices is essential to assuring personal autonomy. Though most people would not phrase their own aversion to a transparent society in such academic language, they would likely concur with Professor Alan Westin's conclusion in his seminal *Privacy and Freedom*:

> The autonomy that privacy protects is also vital to the development of individuality and consciousness of individual choice in life . . . . This development of individuality is particularly important in democratic societies, since qualities of independent thought, [and] diversity of views . . . are considered desirable traits for individuals. Such independence requires time for sheltered experimentation and testing of ideas, for preparation and practice in thought and conduct, without fear of ridicule or penalty, and for the opportunity to alter opinions before making them public. The individual's sense that it is he who decides when to "go public" is a crucial aspect of his feeling of autonomy.[195]

Professor Westin was writing in 1967. Privacy advocates should refuse to accept the argument that new surveillance technologies like RFID now mean the only form of privacy that can survive the twenty-first century is one that sacrifices personal autonomy. That is especially true when a transparent society cannot deliver on its own objectives of equality and accountability. Mutuality of access to information will not empower ordinary citizens because, especially with the emergence of complicated data mining applications, corporations will be able to exploit that information much more effectively. "The mere possession of information does not give one power; it is the ability to . . . use the data that matter[s]."[196] A

---

to Privacy, 4 HARV. L. REV. 193 (1890)). In Brin's version of a transparent society, individuals' homes remain safe havens from public surveillance.

[193] *See* Zarsky, *supra* note 189, at 999–1000.

[194] *Id.* at 999 (footnotes omitted).

[195] ALAN F. WESTIN, PRIVACY AND FREEDOM 34 (1967). *See also* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1427–28 (2000) ("We do not need, or even want, to know each other that well. Less information makes routine interactions easier; we are then free to choose, consensually and without embarrassment, the interactions that we wish to treat as less routine. Informational privacy, in short, is a constitutive element of a civil society in the broadest sense of that term.").

[196] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 74 (2004). *See also* Zarsky, *supra* note 189, at 1022 ("In today's technological reality, equal access to information is insufficient, and access to raw data is almost as good as having no access at all. To grasp and analyze the vast amounts of information available, sophistication is now the key. Sophistication will remain unequal in a transparent

transparent society will not make individuals nearly as competent as Wal-Mart in processing information to the point where it can be utilized to draw conclusions about others.[197]

Despite its lack of viability, Brin's vision raises valid concerns about the efficacy of an incremental privacy measure—state-by-state legislation on a technology-specific basis—in meeting the challenge posed by RFID-tagging of consumer goods. RFID-specific legislation is a targeted approach that contributes to privacy protection by enabling consumers to limit the collection of their personal data in ways that are not burdensome and that can be guaranteed by law enforcement. The fact that RFID-specific legislation is not a magic bullet is part of what makes it worthy of privacy advocates' support; in a country with a historically piecemeal approach to privacy laws, state-level RFID-specific legislation is a proposal that has a chance of passage, if it receives the backing missing from the privacy community. It is not a concern that the RFID-specific legislation outlined in this Note will not solve all of the privacy dilemmas posed by RFID, such as how to guard against the abuse of personal information after it has been collected, because RFID-specific legislation is properly understood within the notion of "complementarity": laws, technologies, self-regulations, and consumer initiatives must work together to balance and to substitute for the limitations of each other.[198] The privacy invasions threatened by RFID are stealthy and multifarious and they require calibrated responses.[199]

---

society, as a large segment of the population will face both the lack of tools and the lack of ability, time, and knowledge." (footnote omitted)).

[197] Another criticism of the premise of a transparent society is that the phenomena of the "bystander effect" and "diffusion of responsibility" mean that citizens will not all be watching each other's backs via pervasive monitoring and data sharing because in a situation where no one has a designated duty to get involved, the possibility of anyone actually intervening voluntarily is remote. In addition, prejudices will result in society not being equally attentive to the problems of all individuals. Zarsky, *supra* note 189, at 1008–09. "[T]he vulnerabilities that transparency exposes must be countered by a shift in social norms of responsibility. Sadly, there is no guarantee that such a shift will indeed occur." Zarsky proceeds to detail the deleterious effects a transparent society will have on personal safety, the equitable distribution of resources, autonomous thought, and the possibilities for exceptions and free-riders.

[198] Gallison and Minow explain the idea of "complementarity" through an analogy to automobile safety:

> On the road we rely on hardware (soft dashboards, shatterproof glass, airbags, and seatbelts). We count on laws that restrict speeding, limit alcohol, and channel traffic. And we demand proactive good sense, the right management of desires on the part of drivers as they handle intrinsically dangerous machines: prosaic as it is, courtesy does matter at 65 miles per hour.

Galison & Minow, *supra* note 50, at 287.

[199] An analogy can be made to the war on drugs. It shows that law has limits as a means of social control but that law can also change behavior and that demonstrating a solution is incomplete does not necessarily mean it should be abandoned.

There is no single solution. The national baseline legislation for which the privacy community lobbies might ideally be part of the mixture of defenses that would protect consumers against RFID-related privacy invasions. It would supplement RFID-specific legislation's emphasis on data collection by regulating data use. It would also reinforce RFID-specific legislation because imposing restrictions on the use of properly gathered information is one way to discourage data collection.[200] However, baseline legislation does not warrant the undivided attention of the privacy community that it currently receives; it is politically unrealistic and it does not recognize to the same extent as RFID-specific legislation that the most effective way of giving consumers control over their own information is to empower them not to share it at all. Creative thinkers like Brin should be subsidized because they may one day imagine a more perfect redress for the privacy invasions threatened by RFID and other surveillance technologies,[201] but a transparent society that cannot achieve its own objectives is not the answer.

Privacy advocates ought to prioritize RFID-specific legislation. Though currently neglected as a solution, it has the power to influence the outcome of RFID implementation if adopted in the near term. A law that alerted consumers to the presence of RFID tags and allowed them to dispose of them easily would eliminate some of the most nightmarish RFID scenarios by making consumers less susceptible to profiling and tracking and also to forms of targeted marketing. The impending widespread deployment of item-level RFID tags means that legal boundaries should be established quickly and the best opportunity for that is at the state-level. Vigorous opposition by industry associations like the GMA has thus far defeated state RFID privacy measures, but industry lobbying has not yet met the countervailing force of the privacy community. What is possible has not yet been determined.

Of course, state RFID-specific privacy measures are not per se good policy. State legislators and privacy advocates should be aware of what other values they implicate in drafting their proposals. They should strive for bills that allow experimentation by regulating the way RFID technology is used as opposed to the way it is designed, so that manufacturers can retain the flexibility to enhance RFID technology in ways that benefit retailers and consumers alike. In addition, state legislators and privacy advocates should consider the equitable effects of RFID-specific legislation on consumers and also on retailers. Bills, such as the one introduced in California in 2004, would have tolerated stores not using RFID readers on their floors selling products bearing RFID tags. These bills would have permitted hundreds of tags to continue to enter the world without consumers

---

[200] *See* Froomkin, *supra* note 164, at 1464.

[201] *See also* GARFINKEL, *supra* note 185, at 260–61 (recommending the creation of a permanent federal oversight agency charged with protecting privacy).

being aware of their existence or the options that exist for disabling them. On the other hand, RFID legislation ought not to disadvantage disproportionately small retailers, who cannot implement the hardware and software required to profit from RFID, by forcing them to deal with manufacturers' loose tags. Privacy advocates must work with state legislators to account for the interests of all stakeholders. Once they do so, they can construct legislation that provides consumers with elements of notice and choice in the face of a technology whose surveillance potential is silent but revolutionary, and a background legal regime that offers little assistance. Protecting consumer privacy requires an amalgam of legal and social responses and properly formulated state-level RFID-specific legislation is a vital component.