WHEN BIG BROTHER PRIVATIZES: COMMERCIAL SURVEILLANCE, THE PRIVACY ACT OF 1974, AND THE FUTURE OF RFID

JOHN M. EDEN[1]

ABSTRACT

RFID is a powerful new technology that has the potential to allow commercial retailers to undermine individual control over private information. Despite the potential of RFID to undermine personal control over such information, the federal government has not enacted a set of practicable standards to ensure that personal data does not become widely misused by commercial entities. Although some potential privacy abuses could be addressed by modifying RFID technology, this iBrief argues that it would be wise to amend the Privacy Act of 1974 so that corporations would have a statutory obligation to preserve individual anonymity and respect the privacy preferences of consumers.

INTRODUCTION

¶1 Modern technology is about to dethrone the old adage that '*money makes the world go round*.' In some countries, the more apt adage may very well soon turn out to be '*RFID makes the world go round*.' RFID, shorthand for "radio frequency identification technology," is already being used as a *mandatory* substitute for money in some private establishments in Japan.[2] This simple yet remarkable technology consists of a small microchip, a protective sheath or container, and a miniature embedded antenna; these components taken together are referred to as RFID tags.[3] RFID tags are capable of transmitting electronic-product-code (ePC) information to RFID

---

[1] LLM/J.D. 2006, Duke University School of Law, M.A. 2000, Stanford University, B.A. 1997, Loyola University Chicago. This article has benefited from the helpful guidance of Seth F. Kreimer, David Lange, H. Jefferson Powell, and Jedediah Purdy. Although all remaining errors and misstatements are the author's alone, Erica Platt in particular deserves hearty thanks for many interesting conversations about RFID technology that stimulated some of the principal arguments in this article.

[2] *Tracking Arcade Game Players*, RFID IN JAPAN, Nov. 6, 2004, http://ubiks.net/local/blog/jmt/stuff3/.

[3] KLAUS FINKENZELLER, RFID HANDBOOK: RADIO FREQUENCY IDENTIFICATION AND APPLICATIONS 7 (1999).

readers—devices designed to store, process and archive tag data.[4] Since these tags are often quite small—the most technologically sophisticated variants are now just the size of a grain of rice[5]— it is easy to see why they have been heralded as a fantastic replacement for traditional currency: *if our currency can be embedded in a tiny RFID tag, it will be both difficult to steal, eminently portable, and easy to replace in the event the tag is lost or destroyed.*

¶2 In addition to providing one technological solution to the search for a workable form of "digital money," RFID has also been used to monitor everything from commercial purchases[6] to the physical movements of government officials[7] to the misadventures of naturally curious children.[8] In February of 2005 the U.S. State Department revealed a plan to embed RFID chips in every newly issued U.S. passport, thereby broadcasting on demand the names, addresses, and digitized photos of all American citizens to a database—ostensibly[9] so that borders can be more effectively managed and threats to national security more readily prevented.[10] Data storage and transmission

---

[4] Intermec Technologies Corporation, *RFID Overview: Introduction to Radio Frequency Identification*, FORBES.COM, Jan. 1, 2002, *available at* http://itresearch.forbes.com/data/detail?id=1010607230_712&type=RES&src=TOPRES.

[5] *FDA Approves Computer Chip for Humans*, MSNBC.COM, Oct. 13, 2004, http://msnbc.msn.com/id/6237364/.

[6] Kim Yong-Young, *Radio Chips May Track Bank Notes*, CNET NEWS.COM, May 23, 2003, http://news.com.com/2100-1017-1009155.html.

[7] Peter Lewis, *RFID: Getting Under Your Skin?*, CNNMONEY.COM, Aug. 5, 2004, *available at* http://money.cnn.com/2004/08/05/commentary/ontechnology/rfid/.

[8] Jo Best, *Schoolchildren to be RFID Chipped: Japanese Authorities Decide Tracking is the Best Way to Protect Kids*, SILICON.COM, July 8, 2004, http://networks.silicon.com/lans/0,39024663,39122042,00.htm.

[9] Privacy advocates have suggested that one of the consequences, if not the purposes, of embedding RFID chips in passports is that identity theft and commercial data collectors will have an easier time clandestinely obtaining personally identifying information. It is important, however, to distinguish between the purpose of adopting RFID technology, on the one hand, and the probable effects, desirable and unsavory alike, on the other. *See* Ryan Singel, *American Passports to Get Chipped*, WIRED NEWS, Oct. 21, 2004, http://www.wired.com/news/privacy/0,1848,65412,00.html.

[10] Electronic Passport, 70 Fed. Reg. 8305 (proposed Feb. 18, 2005) (to be codified at 22 C.F.R. pt. 51). In April of 2005, Frank Moss, Deputy Assistant Secretary for Passport Services, said that the federal government was reevaluating its proposed RFID system in light of widespread consensus that the unencrypted personal information embedded in RFID tags could easily be intercepted by nonauthorized third-parties. Kim Zetter, *Feds Rethinking RFID*

functionality, however, is only the beginning. In addition, DeltaTRAK recently announced that it has developed an RFID-based system for detecting food spoilage during transit by monitoring temperature and humidity fluctuations in food containment units.[11] Further, IBM and EPC Global, the most powerful RFID standards-setting organization, recently unveiled a plan to "create a database that contains the life history of a product," thus providing businesses with a new way to streamline business supply chains.[12] All things considered, RFID is a promising technology many of us may soon be using to keep tabs on virtually everything that is important to us—our kids, our finances, our loved ones, and perhaps even our periodically wayward political figures.

¶3 Nevertheless, RFID is also a technology that could easily be abused. For instance, if private companies embedded RFID tags in products deemed dangerous or socially harmful, the implementation of a centralized database of consumer purchasing patterns could be justified to allow the government to track such purchases. This could have the unwelcome effect of subjecting all consumers to suspicionless monitoring; however, it should also be noted that for some products—e.g., firearms and chemicals commonly used to make explosives—RFID could also provide just the kind of highly accurate tracking system that would benefit society. In any event, credible evidence that private companies intend to deploy this new technology as widely as possible is mounting.[13] Moreover, it is also clear from a number of pilot tests in Europe that corporations are eager—without customer consent or authorization—to embed RFID chips in loyalty cards to monitor purchasing habits.[14]

¶4 Under current privacy law, it is unlikely that consumer groups would have the power to prevent private companies from adopting RFID technology for a number of interlocking reasons. First, the Privacy Act

---

Passport, WIRED.COM, Apr. 26, 2005, http://www.wired.com/news/privacy/0,1848,67333,00.html.

[11] *DeltaTRAK Launches RFID Humidity Sensor*, FOODPRODUCTIONDAILY.COM, May 11, 2004, http://www.foodproductiondaily.com/news/news-NG.asp?n=55887-deltatrak-launches-rfid.

[12] Renee Boucher Ferguson, *Dressing Up RFID for Max Appeal*, EXTREMETECH.COM, Nov. 8, 2004, *at* http://www.extremetech.com/article2/0,1558,1722418,00.asp.

[13] *World's Third Largest Retailed Completes Warehouse RFID Implementation*, Information Week, Jan. 20, 2005 (noting that Metro Group, the world's third largest retailer, recently completed an RFID implementation at its largest warehouse in Germany), http://informationweek.com/story/showArticle.jhtml?articleID=57702741.

[14] *See Scandal: The RFID Tag Hidden In METRO'S Loyalty Card*, SPYCHIPS.COM, http://www.spychips.com/metro/scandal-payback.html.

of 1974 ("Privacy Act" or "Act")[15]—the most comprehensive U.S. law pertaining to privacy—does not apply to private entities, but rather only to government agencies or government-controlled corporations.[16] Thus, private corporations are not bound by the fair information practices, open-access rules, and data-ownership principles embodied in the Act.[17] But even if they were, consumer groups would arguably have a difficult time preventing private companies from *gathering* data, since the Act does not *in principle* proscribe data collection but merely proscribes a narrow subset of data *misuse*.[18] Second, constitutional protections are of little use since the type of data that RFID is capable of collecting is publicly ascertainable, and therefore probably not subject to protection under current Fourth Amendment jurisprudence.[19] Third, even in jurisdictions that recognize the torts of intrusion and the appropriation of private facts in consumer contexts,[20] consumers would only be able to recoup damages ex post; tort law is thus of no help in preventing data aggregation per se.[21] This third feature of our privacy regime is

---

[15] 5 U.S.C. § 552(a) (2000).

[16] *Id*. at § 552(a)(1).

[17] James X. Dempsey & Lara M. Flint, *Surveillance, Records & Computers: Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1474 (2004) (pointing out that "[t]he act requires notice to, and consent from, individuals when the government collects and shares information about them").

[18] *Id.* (pointing out that while the "Privacy Act does include a provision that extends its coverage to databases created under government contract," this particular provision "does not include governmental searches of private sector databases already compiled and maintained for other purposes").

[19] *See* Katz v. United States, 389 U.S. 347, 351 (holding that "what a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection").

[20] It is highly unlikely that most jurisdictions would recognize these tort claims in the consumer context. The private facts appropriated usually have to be of an intimate and sensitive nature, strongly suggesting that tort theory is of little use in articulating what is objectionable in the kind of data collection and item tracking that RFID enables. The reason this is so is illustrated nicely by Professor Post's general observation that invasion of privacy tort claims are successful only when "it can be demonstrated that a defendant has transgressed the kind of social norms whose violation would properly be viewed with outrage or affront, and that the function of this relief is to redress 'injury to personality'". Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 962 (1989).

[21] A point of clarification is necessary here. In theory tort law could provide some degree of deterrence, assuming that damage awards available to private citizens for the torts of intrusion or appropriate of private facts were substantial enough to prevent companies from collecting personally identifiable information without customers' consent. But in practice, tort law is highly unlikely to deter

particularly discomfiting given that many of the recent private initiatives designed to mitigate the dangers of data collection through technological solutions have been wholly unsuccessful and fail to embody sound privacy values.[22]

¶5 There are two broad threats to privacy posed by this new technology. First, under our current privacy regime private companies are at liberty to gather, process, and share customer data without obtaining customer consent to specific data aggregation, archival, and sharing policies and procedures.[23] This feature of our privacy regime is

---

private companies because those companies understand that the value of a potential damage award is unlikely to be large enough for a private citizen to justify bringing suit in the first place. There are two reasons that this is so. First, common law privacy jurisprudence applicable in these tort cases requires that a breach of a privacy right be "offensive to the reasonable person." W. PAGE KEETON ET AL., PROSSER AND KEETON ON TORTS 117 (5th ed. 1984). As many commentators have recognized, this transforms privacy into a "moving target," and is for that reason an unreasonable, unworkable standard. Some have even suggested that that "ultimate consequence of such an approach may be no privacy at all." Julie E. Cohen, *The Law and Technology of Digital Rights Management: DRM and Privacy*, 18 BERKELEY L. TECH. L.J. 575, 592 (2003). Second, in order to establish a violation of privacy under current tort law one must in most cases show that a private fact was disclosed in a way that caused emotional or psychic distress. It is hard to imagine a court awarding money damages to a plaintiff that claimed her privacy was violated because a company *used*—without disclosing—her private consumer preferences. *See* Randall P. Bezanson, *The Right to Privacy Revisited: Privacy, News and Social Change, 1890–1990*, 80 CALIF. L. REV. 1133 1170 n.111 ("Successful privacy cases have never been legion. And recent experience is, if anything, worse both as to the frequency of successful claims and as to the analytical difficulties associated with rationalizing a favorable result.").

[22] *See* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy*, 2001 STAN. TECH. L. REV. 1, ¶89 (2001) ("[P3P] maps nicely to the anti-regulatory views espoused by industry but not at all to the well-established tradition of privacy protection in law. P3P in the end is an invitation to reject privacy as a political value that can be protected in law and to ask individuals to now bargain with those in possession of their secrets over how much privacy they can afford.").

[23] *See* Andrew J. McClurg, *A Thousand Words are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 65 (2003) ("Large companies like Acxiom, Experian, and R.L. Polk & Co. possess profiles of nearly every American consumer and household. Acxiom's InfoBase profiler collects data from more than 15 million sources and contains demographic information on 95 percent of U.S. households. Experian boasts that its databases cover 98 percent of U.S. households and can contain more than 1000 data items per household. Polk's 'Automotive Profiling System' contains

particularly vexing given that we live in an era in which identity theft is particularly common[24] and extremely hard to prevent[25]; thus control over private data is extremely important. Second, the absence of meaningful regulation of new surveillance technologies, particularly RFID, is having a profound effect on the broader social norms that privacy protects. Private facts about consumer preference patterns are currently treated as cost-free commodities for corporate America: companies need not pay for the privilege of aggregating and using data, nor is consumer consent regarded as necessary because consumer surveillance has already been presented as a common practice that is usually in consumers' best interests.[26]

¶6 This iBrief argues that meaningful statutory regulation is necessary for private-and public-sector RFID programs that collect consumer data for purchase forecasting, preference modeling, and risk profiling. The form that effective regulation should take is a matter of dispute, but two models will be explored, a *control oriented* model and a *choice oriented* approach.[27] Under the *control oriented* model, the Privacy Act should be amended to embody privacy-protecting principles that preserve the values of anonymity, seclusion, and control over certain types of personal information. Under the *choice oriented* model, the

---

demographic and lifestyle information on more than 150 million vehicle owners and 111 million households.").

[24] Timothy O'Brien, *Identity Theft is an Epidemic, Can it Be Stopped?*, N.Y. TIMES, Oct. 24, 2004, *available at* http://www.nytimes.com/2004/10/24/business/yourmoney/24theft.html?ex=1100322000&en=bf4604784fbfd500&ei=5070&oref=login.

[25] *See id.* (suggesting that identity theft may be impossible to prevent since there is no way to anticipate the technical creativity of ID-thieves).

[26] *See* McClurg, *supra* note 23, at 66-7 ("Online, Internet advertising companies such as DoubleClick track the clickstream of Internet users across the World Wide Web, creating detailed profiles of their behavior. By storing small text files called 'cookies' on the computers of persons visiting DoubleClick-affiliated sites, the company has stockpiled profiles of more than 100 million individuals. Consumer profiling is not limited to companies that specialize in data collection. Online booksellers and other retailers profile customers by tracking the products they view or buy online. Telephone companies profile customers based on when, how often, and what numbers they call. Supermarkets profile shopping habits by recording and analyzing purchasing information collected through discount or loyalty club cards. Banks and other financial institutions construct profiles based on personal financial data. The Gramm-Leach-Bliley Act of 1999 allows them to share customer financial data with affiliated companies without restriction and to share it with anyone else if customers do not explicitly opt out of such sharing.").

[27] For a general overview of the difference between control and choice-oriented approaches to informational privacy, *see* Rotenberg, *supra* note 22, at ¶¶62–71.

Privacy Act need only be amended in the most minor way—that is, to require corporations to obtain explicit authorization from consumers before gathering or using their private information. Although both of these approaches toward new regulation could very well involve modifying RFID technology, the status of informational privacy as a public good requires that basic, fundamental control rights be given the imprimatur of law even where technological safeguards serve as part of a meaningful solution.

¶7 This iBrief is segmented into three sections. Part I explores the historical development and current capabilities of RFID. Part II considers the implications of this new technology for privacy. This section focuses on the potential for RFID to serve *in the near future* as the primary tool for tracking physical objects and people; specifically, this section explores the arguments weighing in favor and against the *control* and *choice-oriented* approaches to regulating consumer privacy. Part II ultimately advocates a control-oriented model of privacy protection is advocated in this Part, mainly in light of the potential for mass consumer surveillance to become a central feature of commerce in the near future if decisive legislative action is not taken. Finally, Part III proposes an amendment to the Privacy Act of 1974 and explores the advantages and disadvantages of such an amendment.

I. THE CAPABILITIES OF RFID TECHNOLOGY

¶8 The powerful object identification and tracking capabilities of RFID are made possible by a discovery made just before the outbreak of World War II. Scientists at that time discovered that radio waves can be used to identify specific objects in the physical world if those objects are affixed with unique identifying numbers or codes.[28] As long as an object has a unique number associated with it, accurate identification would be a very simple affair.[29] This discovery proved quite useful in the World War II, since the United Kingdom needed an effective, reliable way to distinguish its own fighter planes from inbound German fighters.[30] RFID fit the bill because it allowed for the reliable, remote identification of objects.[31]

¶9 RFID was never adopted as the standard for object identification. In the 1970s, the bar code—or Universal Product Code (UPC)—became the most widely used method for identifying and tracking objects as they

---

[28] WIKIPEDIA, RADIO FREQUENCY IDENTIFICATION (RFID), http://en.wikipedia.org/wiki/RFID (last visited Aug. 25, 2005).
[29] *Id.*
[30] *Id.*
[31] *Id.*

passed through commercial channels.[32] UPC labels were never the ideal technology for managing supply chains and monitoring inventory, for three simple reasons: 1) the labels themselves are easy to disfigure or disable, 2) UPCs must be read at a certain angle, slowing down the monitoring process considerably, and 3) UPCs are typically read sequentially—meaning that multiple UPC labels cannot be read simultaneously.[33]

¶10 RFID is a much more robust technology. While RFID tags can be disabled through physical abuse or destruction, they need not be read at an angle and they can be read simultaneously. The typical system includes tags, an antenna, and a reader or scanner.[34] Tags, usually miniature silicon chips affixed to micro-antennae, come in two varieties—active and passive.[35] Active tags contain a power source that enables them to send data without being prompted by a reader; passive tags cannot transmit data themselves but are merely read by local reading devices.[36] Active and passive tags usually have read-write capability, a feature that is extremely appealing given the advent of the electronic product code (ePC). The ePC is a 96-bit numerical code saved onto the RFID tag itself, and is best viewed as an extension of the current UCC-12 protocol for naming and tracking objects globally.[37] The advantages of using RFID tags in conjunction with the ePC are numerous: not only can these small, often unnoticeable tags be logged without cumbersome physical manipulation, most RFID systems can read ePC numbers through fog, snow and even paint so long as the tags themselves are within standard read range.[38]

---

[32] *Checkout Lines Could Become History*, USATODAY.COM, http://www.usatoday.com/news/science/stuffworks/2001-04-24-smart-labels.htm (last visited Aug. 25, 2005).

[33] WIKIPEDIA, UNIVERSAL PRODUCT CODE, http://en.wikipedia.org/wiki/Universal_Product_Code (last visited Aug. 25, 2005).

[34] Intermec Technologies Corporation, *RFID Overview*, *supra* note 4, at 3.

[35] Active tags are generally larger, more expensive, and have a longer read range. Passive tags, on the other hand, are often very small, inexpensive, and offer long operational life. *See* WIKIPEDIA, *supra* note 28, at *Types of RFID TAGS*.

[36] The Association of the Automatic Identification and Data Capture Industry, *Draft Paper on the Characteristics of RFID Systems*, AIMGLOBAL.ORG, July 2000, http://www.aimglobal.org/technologies/rfid/what_is_rfid.asp.

[37] Mark Roberti, *ePC Networking on Display*, RFIDJOURNAL.COM (May 24, 2004), http://www.rfidjournal.com/article/articleview/957/1/1/.

[38] Some RFID chips can be temporarily disabled by enveloping them in Mylar fabric or by placing a metal plate between the chips and a reader. Josh McHugh,

¶11 ODIN Technologies, an RFID systems integrator based in Reston, Virginia, recently released a comprehensive performance study of eight different tag-types.[39] The study revealed what many industry analysts had been expecting to hear: the best passive tags can be read from multiple angles and while moving at considerable speed—from 600 to 1200 feet per second.[40] Yet even though passive tags can be read very quickly, they generally cannot be read from very far away unless they operate on the higher frequencies. High frequency tags can currently be read from up to 3 or 4 meters away,[41] though in the near future technological improvements will make it feasible to read high frequency tags from a greater distance.[42] RFID is thus an extremely powerful technology that allows for the quick and accurate identification of physical objects—from foodstuffs to clothing to electronic gadgets. To get a sense of just how powerful this technology is, imagine for just a moment a machine that could instantly identify the origin, cost, and properties of every consumer item carried (electronic gadgets, e.g.), worn (clothing, e.g.), or consumed (food and drink, e.g.). That machine is RFID. And the technology to make that machine exists today, right now.

¶12 The potential range of uses for RFID technology is hard to predict at this nascent state of development. But there are a number of important uses already underway:

> 1. GENERAL TRACKING AND SECURITY PURPOSES: Tagging airline baggage, prisoners, cars for tollways,[43] and tagging at the pallet level all goods and products destined for delivery to the U.S. Department of Defense.[44]

A Chip in Your Shoulder, SLATE.COM, Nov. 10, 2004, http://slate.msn.com/id/2109477/.

[39] Catherine O'Connor, *ODIN Benchmarks RFID ePC Tags*, RFIDJOURNAL.COM, Oct. 21, 2004, http://www.rfidjournal.com/article/articleview/1199/1/1/.

[40] *Id.*

[41] *The Magic of RFID: How it Works*, ACMQUEUE.COM, Oct. 2004, http://www.acmqueue.com/modules.php?name=Content&pa=showpage&pid=216&page=2.

[42] *See id.* (pointing out that advances in silicon chip conductivity will allow high frequency tags to be read from farther away in the future).

[43] Karen Dearne, *Radio Tags Take to the Plains*, AUSTRALIANITNEWS.COM, Nov. 9, 2004, http://australianit.news.com.au/articles/0,7204,11302583%5E15841%5E%5Enbv%5E,00.html.

[44] Darrell Dunn, *Defense Department Delays RFID Deadline Until At Least February*, INFORMATIONWEEK.COM, Nov. 12, 2004, http://www.informationweek.com/story/showArticle.jhtml?articleID=52601247.

> 2. ANTI-FRAUD MEASURES: Combating drug counterfeiting in the pharmaceuticals industry.[45]
>
> 3. STREAMLINING BUSINESS PROCESSES: Improving inventory control and reducing inefficiencies in the drug industry due to overstocking or expiry.[46]
>
> 4. CURRENCY SUBSTITUTES: Providing a substitute for regular money.[47]
>
> 5. BORDER SECURITY: Ensuring that low-risk individuals are able to safely traverse major international borders.[48]
>
> 6. ENVIRONMENTAL INTEGRITY: Creating new ways of ensuring that toxic substances are not illegally dumped into the environment.[49]
>
> 7. HUMAN MONITORING: Establishing new methods for track the movements and behavior of children.[50]

Each application of RFID has the potential to be beneficial by increasing safety and accountability, as well as the potential to violate forms of privacy worth protecting.

¶13 The most recent controversy over RFID emerged when the FDA announced its approval[51] of the VeriChip, an implantable device carrying a unique key that hospitals and other health-care providers could use to instantaneously access medical records in an emergency situation.[52] Privacy advocates responded to this new development by pointing out a host of potential problems with implanting such a chip: 1) VeriChip is

---

[45] Martin Downs, *Counterfeit Drugs: A Rising Public Health Problem*, WEBMD.COM, http://my.webmd.com/content/Article/95/103346.htm.
[46] *See* Dearne, *supra* note 43.
[47] *See Tracking Arcade Game Players*, *supra* note 2.
[48] *Nexus: Life in the Fast Lane—RFID Powers Border Crossing Program*, AIMGLOBAL.ORG, May 15, 2004, http://www.aimglobal.org/members/news/templates/casestudies.asp?articleid=134&zoneid=25.
[49] *Japan: Radio Tags Drafted for Eco-compliance*, CNETASIA.COM, http://asia.cnet.com/news/systems/0,39037054,39186726,00.htm.
[50] *See* Best, *supra* note 8.
[51] Letter of Evaluation, Office of Device Evaluation of the Center For Devices and Radiological Health, VeriChip ™ Health Information Microtransponder System (Oct. 12, 2004), *available at* http://www.sec.gov/Archives/edgar/data924642/000106888004000587/ex99p2.txt.
[52] *See* McHugh, *supra* note 38.

not medically safe[53]; 2) the potential for unauthorized access to medical records is a serious drawback of the system[54]; and 3) without effective regulation prior to the wide-implementation of these implants, the likelihood of invasive data aggregation, improper violations of anonymity, and other violations of personal privacy is very high.[55]

¶14 Of course, critics of RFID technology often overlook or intentionally downplay the fact that extremely Orwellian RFID systems would require an integrated network of readers in addition to the ubiquitous affixation of tags. For an individual's personally identifiable information to be transparent, tags must be 1) affixed to physical objects, 2) close enough to readers to transmit whatever information they contain, and 3) not covered by fabric or obscured by other materials that interfere with data transmission. But such critics accurately portray RFID as a technology that in its current and prospective uses represents a way for corporations to keep tabs on its clientele without any *pro tanto* benefit for ceding personal data.

II. UNDERSTANDING WHAT RFID MEANS FOR CONSUMER PRIVACY

¶15 If RFID were to become pervasive, it would certainly be one of the most powerful *single* modalities of surveillance. Where video surveillance is hobbled by the current limitations of facial recognition technology, even passive RFID tags could allow for accurate identification of individuals in a reader-rich environment.[56] Where paying cash for consumer purchases allows one to avoid leaving an electronic trail for interested parties to investigate, RFID may in Europe soon be embedded in currency, leaving no option for the privacy-conscious consumer who wants her purchases to remain anonymous.[57] And where individual credit card companies are only able to analyze and

---

[53] *See* Letter of Evaluation, *supra* note 51, at 3 ("The potential risks to health associated with the device are: adverse tissue reaction; migration of implanted transponder; compromised information security; failure of implanted transponder; failure of inserter; failure of electronic scanner; electromagnetic interference; electrical hazards; magnetic resonance imaging incompatibility; and needle stick.").

[54] *Electronic Privacy Information Center (EPIC) VeriChip Page*, EPIC.ORG, *at* http://www.epic.org/privacy/rfid/verichip.html (last visited Aug. 25, 2005).

[55] *FDA Approves Computer Chip*, *supra* note 5.

[56] However, hardware-based object recognition technology has recently seen significant advances, allowing commercially available cameras to track basic motion, the appearance and movements of objects—including people, animals and automobiles. Donna Howell, *Video Surveillance Develops Sharper Sight*, INVESTOR'S BUSINESS DAILY, Oct. 20, 2004, at A04.

[57] Winston Chai, *Euro Notes May Be Radio Tagged*, ZDNETUK.COM, May 22, 2003, http://news.zdnet.co.uk/business/0,39020645,2135074,00.htm.

assess data about the purchases you make with your particular credit card, a well-designed RFID reader-environment could very well assemble a comprehensive picture of your purchasing preferences.[58] For example, a store equipped with a number of strategically placed RFID readers could assemble a portrait of a particular consumer's preferences by tracking what items she selected while in the store and then making special offers on the basis of that portrait at the checkout counter. Given that RFID readers have recently been miniaturized, it is not difficult to imagine companies—particularly businesses like Target and Walmart—placing RFID readers at store entrances and exists, and at strategic points along store aisles for targeted-advertising purposes.[59]

¶16 Even without a reader-rich environment, RFID is an especially invasive technology because it threatens to make it extremely easy for companies to gather, archive and utilize private data in three ways. First, embedding RFID tags in consumer goods allows companies to learn precisely what customers are buying by conditioning discounts and special offers upon revealing personal information that a consumer would otherwise want to remain private.[60] As noted above, such knowledge allows for highly efficient targeted-advertising, which some regard as an annoyance and others as a significant invasion of privacy. Regardless of whether such advertising is regarded as invasive by a particular customer, the lack of privacy protection represents an unfair burden on privacy-conscious consumers: to object to RFID-enabled consumer surveillance, customers would have to forfeit the benefits associated with purchasing items from a particular store or carrying a tagged discount card. In other words, even if RFID readers only appear

---

[58] This is one way of conceptualizing the threat that RFID technology poses to consumer privacy. However, even the U.S. Government Accountability Office has recognized the genuine threat RFID poses to the confidentiality of consumer information. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, INFORMATION SECURITY: RADIO FREQUENCY IDENTIFICATION TECHNOLOGY IN THE FEDERAL GOVERNMENT, GAO-05-551 21 (May 2005) ("Profiling is the reconstruction of a person's movements or transactions over a specific period of time, usually to ascertain something about the individual's habits, tastes, or predilections. Because tags can contain unique identifiers, once a tagged item is associated with a particular individual, personally identifiable information can be obtained and then aggregated to develop a profile of the individual.")

[59] See *World's Smallest RFID Reader Developed in UK*, FERRET.COM, Dec. 6, 2004, (reporting that the UK-based company Innovation Research & Technology has developed a 12mm by 2mm fully-operational RFID reader) *available at* http://www.ferret.com.au/articles/6d/0c029a6d.asp.

[60] For the purposes of this iBrief I assume, without providing an independent argument, that social policy should be designed with the privacy-conscious consumer in mind.

in department and outlet stores, the perceived and real costs of opting-out will be enough to coerce customers—customers who would otherwise not want their purchasing patterns archived—to accept this new technology on whatever non-negotiated terms retailers offer.

¶17 Second, and closely related to the first objection, under extant privacy law companies could offer an opt-out policy but then lawfully shift the costs of opting out of a scheme like RFID to non-consenting consumers. This could be done in a number of ways. For example, companies already offer discount cards to customers that provide personal information. The cost of offering discounts could be offset by customers who opt-out of RFID-enabled discount programs. Alternatively, mathematical forecasting models could predict the expected economic impact of (1) opt-out rates on RFID-card discount programs and (2) item-level tagging on gross revenues to spread the costs—i.e., expected diminution in sales—of adopting RFID by increasing the price of goods.[61] In short, current privacy law allows companies to sidestep consumer resistance to RFID with the help of economic forecasting.

¶18 Third, since increased advertising has a marked effect on purchasing patterns,[62] and advertising generally is subject to protection under the First Amendment, existing privacy law actually *subsidizes* corporate speech where RFID is utilized as a technique for enhancing marketing efforts. Privacy law subsidizes corporate speech because the technologies of advertising—in this case RFID—are paid for, in one way or another, by customers, and not by the private interests who benefit from those new advertising methods.[63] To be sure, privacy law does not have the effect of subsidizing corporate speech (advertising) in cases where the costs of marketing methods is not borne by a company's target market. But in cases where such costs are shouldered by consumers, corporate speech is certainly being subsidized. Put another way, if meaningful legislation giving consumers an opt-in right is not enacted,

---

[61] Here it is important to note that economists would insist that the survival of RFID depends critically on whether it does lower the cost of distributing goods. Whether RFID would in all industries is beyond the scope of this iBrief; suffice it to say that many large retailers currently assume that RFID will reduce the costs of distributing goods and should therefore be adopted.

[62] *See generally* Daniel Hays Lowenstein, *Commercial Speech and the First Amendment: "Too Much Puff": Persuasion, Paternalism, and Commercial Speech*, 56 U. CIN. L. REV. 1205, 1215–17 (1988).

[63] To the best of my knowledge, the argument that current privacy law subsidizes corporate speech by not providing a mandatory opt-in option for consumers has not been made by any of the academic critics of RFID technology.

private companies could, without abrogating any law or legal principle, stealthily cajole consumers into supporting marketing efforts designed, ironically, to induce those very same consumers to spend more money.

¶19 This discussion assumes, of course, that the terms offered will be unsavory to the privacy-conscious consumer. In practice, this may not always be the case. However, the argument of this iBrief does not turn on empirical facts about how many private companies are likely to provide a quid pro quo that privacy-conscious consumers find unappealing. Rather, the argument here turns on whether consumers should have to cede even more information to private companies than they already do. Critics of this argument could argue that consumers already give away much private information to private companies through opting-in to discount-card programs at retail outlets. There is some truth to this, and indeed it would be odd to claim that the privacy threats posed by ordinary discount-cards and RFID technology are radically different. Nevertheless, there are two powerful ripostes to this criticism. First, because RFID tags are embedded in objects customers cannot decide in a particular circumstance to retain their privacy—as they surely can with discount-cards by not using them at the cash register. Second, a technological standard for RFID tags is likely to emerge in the near future that would allow retailers to "read" the RFID tags of other retailers, thus learning the consumer preferences of their competitors' customers without the permission of those customers. In short, RFID is a technology that provides retailers a way to avoid ever asking their customers to provide any consent whatsoever to commercial monitoring practices.

¶20 Given that (1) consumers are not provided with the choice to opt-in, (2) there are no safeguards in place to prevent companies from passing on the costs of RFID to consumers, and (3) the lack of such safeguards amounts to a mandatory subsidy of commercial speech, a control-oriented approach should be adopted in amending the Act. A control-oriented approach would enhance consumer autonomy by providing an opportunity for consumers to opt out and it would prevent companies from passing on the costs of RFID to consumers in a furtive effort to subsidize commercial marketing efforts. In other words, a well-crafted amendment would address each of the three concerns previously examined.

III. EAST COAST V. WEST COAST CODE: HOW SHOULD RFID BE REGULATED?

¶21 Privacy law scholars familiar with technology have traditionally made a distinction between 'East Coast' code, that is, legal regulations that govern access to personal information, and 'West Coast' code, that

is, the body of rules and constraints built directly into a particular technology. Both types of code can be helpful in regulatory contexts, and each has its own virtues and demerits. But even though West Coast code is sometimes helpful in protecting liberal democratic values—including privacy, free speech and personal dignity—in many instances this code will not effectively protect our values if not induced by law, by East Coast code, to do so.[64]

¶22 Complicating this picture somewhat is the fact that EPCglobal, (formerly known as the Auto-ID center[65]), a research consortium consisting of 5 major universities and over 100 private companies, has suggested that all RFID devices affixed to consumer goods include a kill switch.[66] This switch would deactivate the tag immediately after a purchase was completed, thereby making it impossible for companies to learn the origin, price, and unique identification number of clothing items, personal electronic devices, and other objects owned by customers.[67] Privacy initiatives such as these are certainly well-intentioned, and the technological fixes they suggest are often quite reasonable. But these initiatives share a common weakness: *private companies are not bound to abide by principles they voluntarily adopt*.

¶23 Current privacy law consists of federal laws and regulations—including the Privacy Act of 1974 ("Act"),[68] the Electronic Communications Privacy Act of 1986[69] ("ECPA"), the Fair Credit Reporting Act of 1970[70] ("FCRA") and the Health Insurance Portability and Accountability Act[71] ("HIPPA")—as well as private tort law. Subsection A examines whether existing federal regulations and private tort law are sufficient to address the privacy implications of RFID. Subsection B introduces a proposed amendment to the Privacy Act, and considers how effective such an amendment might be in preventing RFID abuses.

---

[64] *See generally*, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999) (arguing that West Coast code is often unwilling or unable to protect core liberal values, including privacy and free speech).

[65] The Auto-ID Center is now known as EPC Global, Inc. *See generally* WELCOME TO EPCGLOBAL, INC, http://www.epcglobalinc.org (last visited Aug. 25, 2005).

[66] Paul Boutin, *We Know What You're Buying*, SLATE.COM, Sep. 5, 2003, *at* http://slate.msn.com/id/2087976/.

[67] *Id.*

[68] 5 U.S.C. § 552(a) (2000).

[69] *See* Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522, 2701-2709, 3121-3126 (1988 & Supp. V 1994).

[70] Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681-1681(u) (1994).

[71] Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections 29 and 42 of U.S.C.).

A. The Limits of Extant Privacy Law

¶24 Existing privacy law is not flexible enough to cover potential abuses of RFID. Consider first the federal laws and corresponding regulations that constrain data collection. The Act, as mentioned earlier, does not apply until data or information has been collected.[72] According to the Government Accountability Office, "the Privacy Act is likely to have a limited application to the implementation of RFID technology because the act only applies to the information once it is collected, not to whether or how to collect it."[73] The Act provides citizens a right to review private information collected by government agencies,[74] and a concomitant right to correct misinformation,[75] but the Act does not currently contemplate the myriad dimensions of data privacy implicated by new surveillance technologies.[76]

¶25 The ECPA and the FCRA do not fare any better. The ECPA provides a number of important regulations for electronic communications, including a general bar against peddling personal information culled through electronic transactions.[77] Unfortunately, "information" under the EPCA only refers to the contents of communications; transactional records can lawfully be disclosed, even sold, so long as the purchaser is not the federal government.[78] Thus, while RFID systems capable of recording consumer conversations could very well fall under the ECPA, this statute could not readily be used to prevent companies from culling and sharing transactional data.[79]

---

[72] 5 U.S.C. § 552(a).
[73] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 60, at 23.
[74] 5 U.S.C. § 552(d)(1).
[75] *Id.* § 552(d)(2)-(3).
[76] *See* Jerry Kang, *Informational Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1231 (1998) (arguing that the Privacy Act, and other omnibus privacy statutes, utterly fail to protect data privacy because "they apply only to government action").
[77] 18 U.S.C. 2511(1)(c)-(d); *see also* Kang, *supra* note 76, at 1234 (pointing out that data aggregators cannot "divulge the contents of the communications during transmission or while in storage").
[78] 18 U.S.C. § 2703(c)(1)(A).
[79] The Senate Report accompanying the ECPA makes it very clear that the content of a communication is distinct from the status or existence of the transaction itself. Thus, when the ECPA is read in light of its legislative intent, it is virtually impossible to argue that it prohibits the free sharing of transactional data. S. REP. NO. 99-541, at 13 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3567; *see also* Kang, *supra* note 76, at 1235 ("The upshot of this analysis is that the ECPA constrains a communication provider's exploitation of personal information in only limited ways. Although electronic communications providers to the public must keep the contents of

Similarly, FCRA, would not be of much help. In addition to being designed for a completely unrelated regulatory purpose the FCRA does not even constrain what third-party payment providers can do with sensitive consumer information,[80]and courts have consistently held that such information can be exchanged with impunity as long as a "legitimate business interest" can be identified.[81]

¶26 Robust opt-in rules, however, have been adopted for healthcare information under HIPAA. In fact, HIPAA's privacy rule[82] requires health care providers to obtain explicit consent prior to using or disclosing sensitive health information.[83] The privacy rule is far from toothless, as HIPAA[84] provides for stiff civil and criminal penalties for violations of patients' privacy rights.[85] The privacy rule prohibits the use or disclosure of health information which identifies or can be associated with a particular individual without prior consent, requires that healthcare providers and health-information clearinghouses take reasonable steps to notify individuals of their privacy rights, and requires that a report be made to patients whenever there is an intentional or negligent disclosure of their data.[86] But unfortunately, HIPAA's privacy rule only covers health-care information; it is not a generally applicable privacy law.[87]

¶27 Tort law and Supreme Court jurisprudence have proven disappointing as well. Tort law recognizes four different kinds of privacy violations, including (1) intrusion upon seclusion, (2) public disclosure of private facts, (3) appropriation of name or likeness, and (4) publicity that places another in a false light.[88] Some scholars have

---

communications confidential, they have almost no such obligation regarding transactional records.").

[80] 15 U.S.C. §§ 1581a(d), 1581b(3)(e); *see also Kang, supra* note 76, at 1236.

[81] Oscar H. Gandy, Jr., *Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace*, 1996 U. CHI. LEGAL F. 77, 80 (1996).

[82] Standard for Privacy of Individually Identifiable Health Information, 45 C.F.R. §§ 164.502, 164.506 (2002).

[83] *Id.*

[84] 42 U.S.C. §§ 1320d-5(a)(1), 1320d-6(b) (2000).

[85] *See* Mary L. Durham, *Note, How Research Will Adapt to HIPAA: A View from Within the Healthcare Delivery System*, 28 AM. J. L. AND MED. 491, 500 (2002) ("HIPAA imposes civil penalties of up to $ 25,000 and criminal penalties of up to $ 250,000 or ten years in prison for *every* violation.").

[86] *See* 45 C.F.R. § 164.502 (2001).

[87] *See generally*, Ryan Lowther, *Note, U.S. Privacy Regulations Dictated by EU Law: How the Healthcare Profession May be Regulated*, 41 COLUM. J. TRANSNAT'L L. 435 (2003).

[88] *See* RESTATEMENT (SECOND) OF TORTS §§ 652B, 652D, 652C, 652E (1977).

argued that the first tort—intrusion upon seclusion—could in theory be actionable without a violation of one's physical space.[89] This argument would be specious if applied to RFID: absent federal privacy regulations, the prevalence of RFID tags would probably not be regarded as "highly offensive to the reasonable person,"[90] a requirement for tort liability under the Restatement Second of Torts. In addition, there is no constitutional right to informational privacy, although on one occasion the Supreme Court did come close to endorsing such a right. In *Whalen v. Roe*,[91] a case about whether a state recordkeeping statute violated privacy, the Court cleverly avoided deciding whether there exists a clear right to privacy under the U.S. Constitution.[92] While the majority did intimate that under some circumstances the government may have a constitutional obligation to "avoid unwarranted disclosures,"[93] the Court did not specify what those circumstances might be nor was it willing to extend such hypothetical privacy protections to contexts in which data is collected by private, non-governmental organizations.[94]

¶28 There are a number of advantages to Congressional action recognized by scholars in the broader context of protecting private data from unwanted collection and use.[95] And although privacy consortiums and interest groups periodically resist the efforts of corporations to collect private data, efforts at the federal,[96] state,[97] and local[98] level to

---

[89] Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L.J. 1089, 1106 (1998).
[90] RESTATEMENT, *supra* note 88, § 652B cmt. a, b.
[91] 429 U.S. 589 (1977).
[92] *Id.*
[93] *Id.* at 605.
[94] *Id.*
[95] *See* Kang, *supra* note 76, at 1246–66 (arguing that Congressional regulation is often necessary because market forces alone do not protect privacy to a reasonably acceptable degree).
[96] For examples of general opt-in legislation at the federal level, see Consumer's Right to Financial Privacy Act, H.R. 2720, 107th Cong. (2001); Privacy Act of 2001, S. 1055, 107th Cong. (2001); Unsolicited Commercial Electronic Mail Act of 2001, H.R. 718, 107th Cong. (2001); Online Personal Privacy Act, S. 2201, 107th Cong. (2001); Financial Institution Privacy Protection Act of 2001, S. 450, 107th Cong. (2001); Consumer Online Privacy and Disclosure Act, H.R. 347, 107th Cong. (2001); Unsolicited Commercial Electronic Mail Act of 2001, H.R. 95, 107th Cong. (2001).
[97] For examples of proposals at the state level, see S.B. 1258, 45th Leg., 2d Sess. (Ariz. 2002); Financial Privacy Protection Act of 2002, A.B. 1775, 2001-02 Reg. Sess. (Cal. 2002); H.F. 285, 79th Gen. Assemb., 1st Sess. (Iowa 2001); Consumer Privacy Act, S.B. 2988, 224th Leg. Sess. (N.Y. 2001); Consumer Internet Privacy Act, S.B. 4402, 224th Leg. Sess. (N.Y. 2001); S.B. 1547, 48th Leg., 2d Sess. (Okla. 2001).

adopt opt-in privacy standards for personal data have often failed. The very fact that these efforts have failed evidences not only the political influence that private companies possess, but also the necessity of amending the Act. Congress is, however, aware of the problem. In recent congressional hearings on the privacy implications of RFID, Paula J. Bruening of the Center for Democracy and Technology deftly articulated the importance of enacting sensible privacy protections *before* RFID becomes ubiquitous:

> [I]t is more effective and efficient to begin at the outset of the development process to create a culture of privacy that incorporates sound technical protections for privacy and that establishes the key business and public policy decisions for respecting privacy in RFID use before RFID is deployed, rather than building in privacy after a scandal or controversy erupts publicly.[99]

B. A Privacy Act for the Digital Age

¶29 The Act should be amended to explicitly apply a control-oriented privacy approach to the activities of private corporations and providers of consumer services and goods. This iBrief proposes the following amendment to the Act:

> Under the Privacy Act of 1974, as hereby amended, corporations have a statutory obligation to (1) minimize the amount of data collected and preserve individual anonymity whenever possible, and (2) in contexts where anonymity cannot for technological or administrative reasons be protected, obtain explicit permission from citizens to use (a) personally identifying information for specific purposes disclosed to the consumer and (b) information that aggregates consumer data in ways that threaten

---

[98] For examples of successful legislation at the local level, *see* Contra Costa County, Cal., Code ch. 518-4 (2002) (requiring financial institutions to obtain explicit consumer consent before disseminating private data); Daly City, Cal., Ordinance 1295 (Sept. 9, 2002) (requiring notice and consent prior to the disclosure of private financial information); Daly City, Cal., Ordinance 1297 (Nov. 12, 2002) (same); S.F., Cal., Bus. & Tax Regs. Code art. 20 (2002) (same); San Mateo County, Cal., Ordinance 4126 (Aug. 6, 2002) (regulating the disclosure of confidential consumer information), San Mateo County, Cal., Ordinance 4144 (Nov. 5, 2002) (same).

[99] *RFID Technology: What the Future Holds for Commerce, Security, and the Consumer: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Prot. of the House Comm. on Energy and Commerce*, 108th Cong. 28 (2004) (statement of Paula J. Bruening, Staff Counsel, Center for Democracy and Technology).

> consumer anonymity whenever a new tracking technology is used for a substantially commercial purpose.[100]
>
> Under the amended Act, (3) private companies may not discriminate against consumers who refuse to have their personal information collected via RFID or similar technologies. Private companies may not provide differential services, preference programs, or special incentives despite whatever differential costs are associated with selling goods or providing services to non-consenting consumers that are not associated with selling or providing similar goods or services to consumers who consent to have their personal information archived and used for fully disclosed purposes.

¶30 Provision (1) is the data-minimization principle, necessary to prevent corporate interests from collecting, archiving, using and selling data in a format that violates anonymity. This is the fundamental rule of the amendment, for it stipulates that consumer anonymity is a more important value than targeted advertising. For instance, this provision, when read in conjunction with provision (2), would make it unlawful for Wal-Mart to associate purchase-related data gathered via RFID with specific customers unless explicit consent had been obtained prior to data collection. Notice also that provision (1), when read in conjunction with (2), prohibits collecting *specific types* of data for which a company has not already obtained permission.[101]

¶31 Provision (2) is the opt-in principle, necessary to prevent companies from collecting data surreptitiously from consumers and then using that data in unauthorized ways. This provision has much in common with standard opt-out principles that have already been proposed or promulgated in connection with informational privacy.[102] The main difference between provision (2) and standard opt-out

---

[100] Provision (2) shares some similarities with a bill introduced in the House of Representatives in 2004, commonly referred to as the Opt Out of ID Chips Act. Though never enacted, the Act would have (a) required warning labels on all products carrying RFID tags, and (b) provided consumers with a right to have RFID tags permanently disabled at the time of purchase. *See* H.R. 4673, 108th Cong. (2004), *available at* http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.4673.IH:.

[101] Provision (1) is somewhat similar to Professor Kang's proposed default rule for governing cyberspace transactions: "Such personal information may be processed only in functionally necessary ways" but parties are "free to contract around the default rule." Kang, *supra* note 76, at 1268.

[102] For a good example of a federal statute and regulatory regime based on opt-out principles, *see* the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 502, 113 Stat. 1338, 1437-40 (1999) (codified in scattered sections of 15 U.S.C.) (outlining the obligations of financial institutions regarding the disclosure of personal information).

principles is that companies would have to obtain explicit consent from customers *before* collecting and using their personal data. It is possible that an opt-in provision would make RFID-enabled data collection more expensive, since the costs of data collection would include the time and resources expended to obtain explicit consent.[103] But this is a virtue—not a drawback—of this proposed amendment.

¶32 Provision (3) is the anti-discrimination principle, a provision indispensable to protect consumers from shouldering the cost of opting-out of a data-collection scheme like RFID. For instance, this provision would have the welcome effect of preventing, at least in some cases, companies from offering wildly differential pricing to customers who decided to opt-out of an RFID-discount card program. This is perhaps the most politically controversial aspect of the proposed amendment, because industry advocacy groups would certainly view this provision as a way to stifle completely the "right" of private companies to provide incentives for customers to willingly reveal personal information.

CONCLUSION

¶33 The proposal outlined in this iBrief is modest, pragmatic, and most importantly, proportional to the threat that RFID represents to informational privacy. Nonetheless, it is a proposal that is clearly out of line with our current practices. We are all to ready to disclose private aspects of our lives to commercial entities, too eager to give up forms of anonymity that we would do better to insist upon.[104] Recent trends to trade away privacy protections are often predicated upon misplaced, erroneous notions that technological progress is an unqualified good, a claim grounded in the unchallenged assumption that the technology industry itself is committed to antigovernment libertarianism. [105]

---

[103] *See generally*, Michael E. Staten & Fred H. Cate, *The Impact of Opt-in Privacy Rules on Retail Credit Markets: A Case Stud of MBNA*, 52 DUKE L.J. 745 (2003) (arguing that opt-in rules generally neutralize the many of the efficiency gains obtained through technologically advanced data collection techniques).

[104] Even fervent privacy advocates have accepted the dubious notion that industry-driven controls are preferable to legislative action. *See* Declan McCullagh, *RFID Tags: Big Brother in Small Packages*, CNET.COM, Jan. 13, 2003, http://ecoustics-cnet.com.com/RFID+tags+Big+Brother+in+small+packages/2010-1069_3-980325.html?tag=nl.

[105] JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE 127 (2004) ("The entrepreneurs of Silicon Valley like to think of themselves as antigovernment libertarians, and the business nostrums of the era before the dot-com crash assumed that the Internet would lead inevitably to the end of hierarch and centralized authority and the flourishing of individual

Corporations, whether they are steeped in new technology or firmly grounded in the world of bricks-and-mortar, have never been committed as a matter of principle to something as heady and theoretical as libertarianism. Even well-intentioned private efforts, such as EPCglobal's suggestion that RFID tags be disabled once purchases are made, can be voluntarily disregarded and do not carry the force and legitimacy of law.

¶34 Early international norms governing privacy also failed to take seriously the threat posed by corporate stalking. For instance, in 1950 Article 8 of the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms ("Convention") was adopted, declaring that "everyone has a right to respect for his private and family life" and that "there shall be no interference *by a public authority* with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of a country."[106] Fortunately, international treaties and agreements ratified since the Convention have not echoed its curious assumption that privacy can only be violated by governmental agencies.[107]

¶35 But international privacy norms have been no match for the "wait and see" attitude that businesses benefiting from RFID technology have been selling to the public and legislators alike. For example, a recent California bill[108] designed to set basic and reasonable standards for RFID systems was steamrolled when Hewlett Packard, the American Electronics Association, and the California Grocers Association argued

---

creativity. When the e-businesses technologies of tracking, classifying, profiling, and monitoring were used to identify the preferences of American consumers and to mirror back to each of us a market segmented version of ourselves, Silicon Valley could argue that it was serving the cause of freedom and individual choice.").

[106] Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, Europ. T.S. No. 5 (entered into force Sept. 3, 1953), *reprinted in* 3 INTERNATIONAL LAW & WORLD ORDER: BASIC DOCUMENTS III.B.2 (Burns H. Weston ed., 5 vols., 1994) *available at* http://conventions.coe.int/treaty/en/Treaties/Html/005.htm.

[107] *See* European Convention for the Protection of Individuals With Regard to the Automatic Processing of Personal Data, signed on Jan. 28, 1981, Europ. T.S. 108, 20 I.L.M. 317 (entered into force Oct. 1, 1985); Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *available at* http://www.dataprivacy.ie/6aii.htm.

[108] *See* S.B. 1834, 2004 Leg., Reg. Sess. (Cal. 2004), *available at* http://www.sims.berkeley.edu/academics/courses/is205/s05/Cal%20Sen%20B%201834%20(2004).pdf.

that "premature" regulation would "have unintended consequences" although "[these industry groups] did not elaborate on those consequences."[109] This "wait and see" attitude encourages Congress and the citizenry at large to accept the truly fantastic idea that private corporations will self-regulate a $900 million-dollar market—expected to reach $2.3 billion by 2010—to protect consumer privacy.[110] As one particularly astute citizen recently explained, the public is often hoodwinked into dubious new technology because during its development the associated social costs are either ignored completely or cleverly minimized by private companies:

> In our society, technology advances in a vacuum—the morality and actual usefulness of a product is never considered while a technology is under development; once it is developed, [corporations] assume they have a right that supercedes the rights of all others to make money off a product, regardless of how it affects other people. Marketing merely steps into that vacuum . . . and markets technology without a thought as to its adverse effects.[111]

¶36 This critique exaggerates somewhat the notion that RFID has been developed and marketed 'without a thought as to its adverse

---

[109] Claire Swedberg, *California RFID Legislation Rejected*, RFIDJOURNAL.COM, July 5, 2004, http://www.rfidjournal.com/article/articleview/1015/1/1/. Since SB 1834 was defeated, California lawmakers have introduced the Identity Information Protection Act of 2005, an act that in its original form would have prohibited the use of RFID tags in a range of identification cards in California, including driver's licenses, school ID-cards, and any identification card associated with a government benefit program. *See* S.B. 682, 2005 Leg., Reg. Sess. (Cal. 2005), *available at* http://info.sen.ca.gov/pub/bill/sen/sb_0651-0700/sb_682_bill_20050511_amended_sen.pdf. After strong resistance by the RFID lobby in California, the bill was amended twice to "allow the RFID technology if it contains a unique personal identifier and not personal information, such as an individual's name, address, telephone number, date of birth, Social Security Number or biometric identifier, among others." Dibya Sarkar, *California Lawmakers Soften RFID Stance*, FWC.COM, Jun. 28, 2005, http://www.fcw.com/article89416-06-28-05-Web. Unfortunately, these amendments were not deemed sufficient to justify moving the bill forward by the California Assembly's Appropriations Committee, which recently "decided to sideline the proposed law until next year." Alorie Gilbert, *California Shelves RFID Ban*, ZDNETNEWS, Aug. 26, 2005, http://news.zdnet.com/2100-1009_22-5843867.html.

[110] Tony Hallett, *RFID Becoming Billion-Dollar Market*, SILICON.COM, Apr. 19, 2004, http://hardware.silicon.com/storage/0,39024649,39120064,00.htm.

[111] Letter from Steve Grant, United States citizen, to Declan McCullagh, Chief Political Correspondent, CNET NEWS.COM (Aug. 30, 2004), http://news.com.com/5208-1039-0.html?forumID=1&threadID=1979&messageID=10303&start=-1.

effects.' Many RFID applications will undoubtedly have a direct, positive impact on human health and safety. For example, Applied Digital's VeriChip technology will one allow doctors in emergency contexts to access medical records instantly. Nevertheless, it is worth remembering that new technologies are often embraced not because they are genuinely useful or necessary—but rather because they are already available and ready-to-hand. The amendment proposed in this iBrief has the virtue of allowing consumers a choice: it gives consumers the power to *reflectively* endorse RFID, instead of merely accepting the ubiquity of this technology after large, politically powerful companies have decided that a radio frequency future is the only future.