RELAX, DON'T DO IT: WHY RFID PRIVACY CONCERNS ARE EXAGGERATED AND LEGISLATION IS PREMATURE

Jerry Brito[*]

ABSTRACT

The recent push to replace UPC barcodes on all consumer goods with RFID tags has resulted in a backlash by privacy activists. Legislation to regulate RFID technology has been introduced in several states. Such regulation could stunt this fledgling technology. While some concerns might have merit, most are exaggerated. This is so especially because the tracking capabilities of RFID have been overstated by both its detractors and proponents. Before we regulate, we should first confirm that privacy fears are not baseless and will not be constrained by market forces. We should be more concerned by government use of RFID—something to which privacy advocates have paid little attention.

INTRODUCTION

New technologies reliably rouse old privacy concerns. The newest technology to inflame the passions of privacy advocates is radio frequency identification (RFID). Specifically, an industry movement to replace barcodes on consumer goods with RFID tags has raised concerns that businesses will link individual identities to uniquely numbered items and thereby track peoples' movements. Lawmakers around the country have taken notice and have begun to introduce legislation that would constrain the new technology.

But RFID technology is not as all-powerful as its detractors—or its proponents—claim. Concerns over RFID-equipped burglars and GPS-like tracking capabilities are exaggerated. However, concerns that are more legitimate are a continuation of the debate over the collection

[*] Managing Editor, 2004-05, Federal Circuit Bar Journal; J.D. expected May 2005, George Mason University School of Law; B.A. in Political Science, August 1999, Florida International University. The author would like to thank Lawrence Greenberg and Gerard Stegmaier for helping him navigate the waters of privacy.

of consumer data. RFID is simply the new player in this game and its emergence does not substantively change the existing debate. Nevertheless, proposed regulations aim directly at RFID and, if enacted, could stunt the technology's development.

Part I of this article explains RFID technology and outlines its private and governmental applications. Part II analyzes the concerns espoused in the media and in the legal literature by privacy advocates, and shows that these concerns are overstated. It also notes that while the most legitimate privacy concerns over RFID center on government use and misuse of the technology, activists and legislators have paid relatively little attention to that side of the issue. Part III surveys proposed RFID legislation and explains why regulation is unnecessary given that existing privacy laws and market forces will keep improper uses of the technology in check.

I. RADIO FREQUENCY IDENTIFICATION 101

Radio frequency identification (RFID) systems are a subset of a larger class of technology known as automatic identification (Auto-ID) systems.[1] Other Auto-ID systems include such common technologies as barcodes, smart cards, and optical character recognition systems.[2] The purpose of these technologies is to identify and track people, animals, and goods.[3]

[1] Klaus Finkenzeller, RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification (Rachel Waddington trans., John Wiley & Sons Ltd 2d ed. 2003) (1999).

[2] *Id*. at 2-7.

[3] *Id*. at 1.

For example, a bag of potato chips might have a Universal Product Code[4] barcode printed on it. Scanning the barcode with a laser beam at checkout allows a cash register to easily identify the product and ring the correct price. Behind the scenes, the same barcode might be printed on cases or palettes of the potato chips. Scanning the code at different points in the supply chain helps producers, distributors, and retailers manage inventories and track deliveries. Similarly, a smart card might give someone access to a building by identifying the person at the main door. The same identification process can track which doors the person unlocks within the building and at what time. Such an automated identification system could also be programmed to open only certain doors depending on whose card is presented.

While a barcode requires line-of-sight scanning, and smart cards require physical contact with a reader, RFID-tagged objects can be identified at a distance.[5] Not only is this more convenient, but a contactless design also results in less wear and tear.[6] RFID systems are also faster and more secure than other Auto-ID technologies.[7] Even though RFID tags were invented in 1969 and patented in 1973, the technology is only now becoming technologically and commercially viable.[8]

[4] The Uniform Code Council, a nonprofit standards-setting body, developed the Universal Product Code (UPC) in the 1970s. The UPC was first a tool for grocery supply-chain control and checkout but soon spread to all parts of commerce. In 1974, an ad-hoc committee in Europe developed a UPC-compatible code called the European Article Numbering (EAN) system. Today, the system is known as the "EAN.UCC System" and is managed by the UCC and EAN International. UCC joined the EAN. http://www.uc-council.org/ean_ucc_system/stnds_and_tech/eanucc-faq.html). *See* UNIFORM CODE COUNCIL, THE UNIVERSAL PRODUCT CODE, *at* http://www.uc-council.org/upc_background.html (last visited June 22, 2004); EAN INTERNATIONAL, ABOUT EAN INTERNATIONAL – HISTORY, *at* http://www.ean-int.org/history.html (last visited June 22, 2004).

[5] FINKENZELLER, *supra* note 1, at 8.

[6] *Id*. at 7-8.

[7] *Id*. at 8.

[8] Mario Cardullo, *Genesis of the Versatile RFID Tag*, RFID JOURNAL, *at* http://www.rfidjournal.com/article/articleview/392/1/2/ (last visited June 14, 2004).

A. How RFID Systems Work

RFID systems have two main components: a transponder and a reader.[9] Transponders are the data-carrying device in an RFID system and are usually referred to as RFID tags.[10] The transponder is affixed to the object to be identified—anything from a bag of potato chips to a contactless smart card key.[11] The reader is a radio transceiver that communicates with the transponder via radio waves.[12] RFID tags are tiny chips composed of an electronic circuit attached to an antenna.[13] They can be as small as 0.3 millimeters square—about half the size of a grain of sand.[14] The electronic circuit of an RFID tag has memory where data can be stored.[15] RFID tags are always listening for radio signals sent by RFID readers.[16] When a transponder receives a certain radio query, it responds by transmitting the unique ID code stored in its memory back to the reader.[17]

[9] FINKENZELLER, *supra* note 1, at 7.

[10] ACCENTURE, RADIO FREQUENCY IDENTIFICATION (RFID) WHITE PAPER (2001), *available at* http://www.Accenture.com/xdoc/en/services/technology/vision/RFIDWhitePaperNov01.pdf.

[11] *Id*.

[12] *Id*.

[13] *Id*. at 2.

[14] RFID Journal, *Hitachi Unveils Smallest RFID Chip* (Mar. 14, 2003), *at* http://www.rfidjournal.com/article/articleview/337/1/1/ (last visited Oct. 13, 2004).

[15] ACCENTURE, *supra* note at 2.

[16] Scott Granneman, *RFID Chips Are Here*, SECURITY FOCUS, *at* http://www.securityfocus.com/columnists/169/ (June 26, 2003).

[17] *Id*.

RFID tags can be active or passive.[18] Active tags have batteries that provide them with power, while passive tags do not.[19] Having a battery allows an active tag to broadcast its signal farther than a passive tag and reduces the reader's power requirements.[20] Passive tags are powered by the radio signals from the reader that wakes them and requests an answer, but this means that their broadcast range is relatively short and that they require higher-powered readers.[21] Active tags are necessarily bulkier than passive tags, so the smallest RFID tags are passive.[22] The batteries on active tags last from two to seven years and add significantly to the cost of the tags, while passive tags last up to twenty years and are relatively inexpensive.[23]

RFID tags also operate at different frequencies, which determine their broadcast range and data transfer speed.[24] RFID systems are classified as low- and high-frequency systems.[25] Low-frequency tags are used for applications that require shorter read ranges like security access

[18] INTERMEC TECHNOLOGIES CORPORATION, RFID OVERVIEW: INTRODUCTION TO RADIO FREQUENCY IDENTIFICATION (1999), *available at* http://whitepapers.informationweek.com/detail/RES/1010607230_712.html. ("Historically, an RFID device that did not actively transmit to a reader was known as a tag. An RFID device that actively transmitted to a reader was known as a transponder (TRANSmitter + resPONDER). However, it has become common within the industry to interchange the terminology and refer to these devices as either tags or transponders.")

[19] ACCENTURE, *supra* note, at 3.

[20] *Id*.

[21] *Id*.; Granneman, *supra* note 16.

[22] ACCENTURE, *supra* note, at 3.

[23] *Id*.

[24] *Id*. at 5. Specifically, the common passive RFID tags and their characteristics are:

> Low Frequency RFID systems operate at about 125 kHz with a typical maximum read range of up to 20 inches (508 mm). High Frequency RFID systems operate at 13.56 MHz with a typical maximum read range of up to 3 feet (1 meter). Ultra-High Frequency RFID systems operate at multiple frequencies, including 868 MHz (in Europe), a band centered at 915 MHz, and 2.45 GHz (microwave). Read range is typically 3 to 10 feet (1 to 3 meters), but systems operating in the 915 MHz band may achieve read ranges of 20 feet (6 meters) or more.

ZEBRA TECHNOLOGIES, RFID: THE NEXT GENERATION OF AIDC APPLICATION WHITE PAPER 2 (2004), *available at* http:// www. Accenture.com/xdoc/en/services/technology/vision/RFIDWhitePaperNov01.pdf.

[25] ACCENTURE, *supra* note, at 5.

keys, inventory management, checkout scanning, and payment systems.[26] High-frequency systems are used for applications that require longer read ranges, such as highway toll-collection and cargo container tracking.[27] While high-frequency tags transmit data faster and can be read from farther away, they also consume more power and are more expensive than low-frequency tags.[28]

Finally, RFID tags can be read-only, read-write, or a combination in which some data (such as a serial number) is permanently stored, while other memory is left for later use.[29] For a tag to be read-write, it generally must be active and have its own power source.[30] Read-only tags are typically passive and are pre-programmed with a unique set of data (usually 32 to 128 bits) that cannot be modified.[31] Read-only tags most often operate as a "license plate" much like barcodes.[32] The "license plate number," when scanned into a computer, will correspond to an entry in a database containing modifiable product-specific information.[33]

RFID readers are made up of one or more antennas used to send and receive information from tags, and a processor to decode received data.[34] Collected data is passed via cable or Wi-Fi

[26] Kendra Mayfield, *Radio ID Tags: Beyond Bar Codes*, WIRED NEWS, *at* http://www.wired.com/news/technology/0,1282,52343,00.html (May 20, 2002).

[27] *Id*.

[28] *Id*.

[29] ZEBRA TECHNOLOGIES, RFID: THE NEXT GENERATION OF AIDC APPLICATION WHITE PAPER (2004), *available at* http://www.zebra.com/whitepapers/11315Lr2RFIDTechnology.pdf.

[30] AIM GLOBAL, WHAT IS RADIO FREQUENCY IDENTIFICATION (RFID)? *at* http://www.aimglobal.org/technologies/rfid/what_is_rfid.asp (June 14, 2004).

[31] *Id*.

[32] *Id*.

[33] *Id*.

[34] ZEBRA TECHNOLOGIES, *supra* note 29, at 2.

to a host computer system running identification or tracking software.[35] Readers can be portable or they can be fixed and positioned at strategic points, such as dock doors or points on an assembly line, where they will be able to identify the tags that come into their range.[36]

This paper will focus on passive, low frequency, read-only RFID tags, because these are the tags currently being considered for widespread commercial use. They are the smallest and cheapest type of tags, and they meet the requirements of most commercial applications, including consumer product tracking—the use that has raised the most privacy eyebrows.

B. Applications of RFID Technology

Imagine you are shopping on Fifth Avenue. You walk into a boutique and look around for a new dress. A sales clerk notices you eyeing a particular red number and says he would like to tell you more about it. He takes a handheld device that looks much like a PDA and points it at the dress. An instant later, flatscreens light up to show video of a model in the dress sashaying on a catwalk in Paris. Designer sketches and color swatches also appear and you notice a shade of blue that you like. Looking at his handheld for just a moment, the clerk confirms that the dress in blue, and in your size, is in stock; he'll have someone bring it out.

Shoppers at the New York flagship store of Italian fashion house Prada did not have to imagine; such an experience was made possible using RFID.[37] Every garment, shoe and bag in the store was tagged with an RFID chip.[38] Handheld devices were linked to a real-time

[35] *Id*.

[36] *Id*.

[37] RFID Journal, *Learning from Prada*, *at* http://www.rfidjournal.com/article/articleview/272 (June 24, 2002); IDEO, PRADA CASE STUDY, *at* http://www.ideo.com/case_studies/prada.asp (June 15, 2004).

[38] *Id*.

inventory system to let clerks know what colors and sizes were stocked.[39] Dressing rooms had RFID-reader-equipped racks on which customers could hang the clothes they wanted to try. The racks knew which garments had been selected and displayed interactive information about them on the dressing room's touchscreen.[40]

This high-tech gadgetry can mean not just convenience for the customer, but also increased sales for the retailer. Less-exclusive retailer the Gap has found that it can increase sales in RFID-equipped stores by 7 to 15 percent by freeing sales staff to spend more time with customers and less time in the stockroom.[41] Although the Prada über-tech experiment was ultimately not completely successful,[42] other retailers, including Abercrombie & Fitch, plan to roll out new RFID stores.[43] And while most of the buzz surrounding RFID is in the private sector, government agencies are taking note of the technology.[44]

1. Commercial Applications of RFID

Less exotic commercial applications of RFID already surround us. One of the most popular uses of RFID is the Mobil Speedpass payment system. Users are given a keychain fob with an embedded RFID tag that is programmed with a unique ID number.[45] That number—

[39] *Id*.

[40] *Id*.

[41] *Id*.; *See also* Cate T. Coran, *Abercrombie To Give RFID A Try*, WOMEN'S WEAR DAILY, May 18, 2004 at 24.

[42] Greg Lindsay, *Prada's High-Tech Misstep*, BUSINESS 2.0, Mar. 2004, *available at* http://www.business2.com/b2/subscribers/articles/print/0,17925,594365,00.html (explaining how two years later, the technology at the New York Prada store goes unused largely because of employee and customer apathy). *See also* Joseph Tarnowski, *No tech for tech's sake*, PROGRESSIVE GROCER, Apr. 1, 2004, at 3, *at* 2004 WL 67671223 (opining that Prada's failure may have been caused by foisting on consumers technology they were not ready for).

[43] Cate T. Coran, *Abercrombie To Give RFID A Try*, WOMEN'S WEAR DAILY, May 18, 2004, at 24.

[44] *See* section I.B.2 *infra*.

[45] EXXONMOBIL, SPEEDPASS: HOW IT WORKS, *at* http://www.speedpass.com/how/index.jsp (last visited Oct. 13, 2004).

which is meaningless to anyone else—is associated with the user's payment information in Mobil's database, including a credit card number.[46] To make an effortless payment, the user only has to wave the fob in front of an RFID reader at the gas pump or the register.[47]

Similarly, several public transit systems have begun issuing payment cards embedded with RFID.[48] Using kiosks or direct deposit, commuters periodically add funds to their account, which is in turn associated with the unique number in the RFID card.[49] Subway turnstiles are equipped with RFID readers, and waving your card in front of them lets you in and deducts the appropriate fare from your account.[50]

Delta Air Lines is leading the way to track passenger bags using RFID. Current tracking systems rely on barcodes affixed to bags with adhesive labels, but these need to be manually scanned. Delta is testing a system that would embed RFID tags in the printed labels to allow baggage tracking using RFID readers placed at strategic points, including luggage carousels.[51] Today, if a passenger bag is misdirected, airlines struggle to identify the specific lost bag, which might have been sent anywhere in the country. By using RFID, Delta hopes to be able to

[46] *Id*.

[47] While the SpeedPass system only works at Mobil and Exxon gas stations, along with a few retailers in certain geographic areas, other RFID payment systems are entering the market. Credit card companies have been working on a standard for contactless card readers, and MasterCard and American Express have already begun field tests of their RFID cards, which they say are more secure than today's cards. Associated Press, *Wave the Card for Instant Credit*, *at* http://www.wired.com/news/technology/0,1282,61603,00.html (Dec. 14, 2003).

[48] Transit systems that have adopted RFID include Chicago, New York, San Francisco, Seattle, and Washington D.C. SMART CARD ALLIANCE, OVERVIEW OF SMART CARD INITIATIVES IN THE TRANSPORTATION INDUSTRY, *at* http://www.smartcardalliance.org/about_alliance/transportation_initiatives.cfm (last visited Oct. 13, 2004).

[49] WASHINGTON AREA METROPOLITAN TRANSIT AUTHORITY (WMATA), *S*MARTRIP: MORE THAN A SMART CARD—IT'S PURE GENIUS., *at* http://www.wmata.com/riding/smartrip.cfm (last visited Oct. 13, 2004).

[50] *Id*.

[51] RFID Journal, *Delta Takes RFID under Its Wing*, *at* http://www.rfidjournal.com/article/articleview/468 (June 20, 2003). *See also* Bruce Mohl, *Radio Tags May Yet Solve the (Costly) Lost Baggage Problem*, BOSTON GLOBE (May 16, 2004), at M7.

pinpoint a bag's location and automatically send a wireless message to a staff person in a position to pull the bag and send it to its proper destination.[52]

There are a plethora of commercial uses of RFID being developed and already on the market.[53] But the one application that has captured the imagination of corporate America—as well as that of privacy activists—is effectively replacing barcodes on consumer goods by tagging every retail product with a uniquely numbered RFID chip.

The goal is to streamline the entire supply chain—from manufacturing to distribution to retailer. Constant, automatic knowledge of inventory levels means reduced warehousing costs and inching ever closer to that state of nirvana known as just-in-time manufacturing.[54] Suppliers could save money by keeping better track of their returnable assets like pallets and containers.[55] The technology also promises to help manufacturers and retailers prevent "backshop" theft, which is estimated to cost companies billions of dollars each year.[56] Identifying whole

[52] RFID Joumal, *Delta Takes RFID under Its Wing*, *at* http://www.rfidjournal.com/article/articleview/468 (June 20, 2003).

[53] RFID has been used to track merchandise, as a cashless payment system, to verify inspectors have followed safety procedures, to replace airline boarding tickets, to track bags at airports, to track railway cars, as anti-theft devices, to track public buses, as a keyless ignition system, and to track rubbish bins. ACCENTURE, *supra* note, at 33-34; to track students at a charter school. Julia Scheeres, *Three R's: Reading, Writing, and RFID*, WIRED NEWS, *at* http://www.wired.com/news/technology/0,1282,60898,00.html (Oct. 24, 2003); To track seniors in need of care. Mark Baard, *RFID Keeps Track of Seniors*, WIRED NEWS, *at* http://www.wired.com/news/medtech/0,1286,62723,00.html (Mar. 19, 2004); To replace ID tags on pets, to track livestock, to facilitate access control, for sports ticketing, and product authentication. Cathy Booth Thomas, *The See-It-All Chip*, TIME (Sep. 22, 2003), at A8, *available at* 2003 WL 58582602.

[54] *See generally* IBM, RFID TAGS: AN INTELLIGENT BAR CODE REPLACEMENT (2001), *available at* http://whitepapers.zdnet.co.uk/0,39025945,60021109p,00.htm.

[55] Mark Baard, *Radio Debut Set for This Week*, WIRED NEWS, *at* http://www.wired.com/news/privacy/0,1848,60408,00.html (Sept. 15, 2003).

[56] VERISIGN, THE EPC NETWORK: ENHANCING THE SUPPLY CHAIN (2004), *available at* http:// http://www.verisign.com/static/002109.pdf. ("Up to $30 billion each year is lost due to theft, often called 'product shrinkage.' The majority of this loss occurs in the middle of the supply chain, for example between the manufacturer's front door and the retailer's back door."). *See also* Associated Press, *Wal-Mart Turns to Smart Tags*, *at* http://www.wired.com/news/technology/0,1282,63290,00.html (Apr. 20, 2004).

shipments of goods automatically upon arrival at a loading dock could save labor all around.[57] As one observer put it, "Wal-Mart would love to be able to point an RFID reader at any of the 1 billion sealed boxes of widgets it receives every year and instantly know exactly how many widgets it has. No unpacking, no unnecessary handling, no barcode scanners are required."[58]

Retailers also expect RFID to result in greater customer satisfaction. "Smart shelves" that keep track of how stocked they are—and that send automatic messages to the storeroom when their level of, say, Tickle Me Elmo dolls gets too low—will ensure that customers always find shelves full.[59] If this information is shared with suppliers, they could be better able to match supply to demand and reduce inventory sellouts.[60] Also, consumer products that are tagged with unique identifying numbers at the item level could enable returns without a receipt, as well as the much-touted self-checkout.[61] Unique identification could also reduce waste during product recalls by pinpointing the few defective items rather than sacrificing a whole batch.[62]

But in order to make these cross-industry benefits possible, the codes that will identify products in the supply chain must be standardized, just like UPC codes are today. That standard,

[57] Associated Press, *supra* note 56. *See also* VERISIGN, THE EPC NETWORK: ENHANCING THE SUPPLY CHAIN 3 (2004), *available at* http://www.verisign.com/static/002109.pdf.

[58] Granneman, *supra* note 16.

[59] *See* Mayfield, *supra* note 26.

[60] FOODPRODUCTIONDAILY.COM, *How manufacturers can benefit from RFID*, *at* http://www.foodproductiondaily.com/news/news-NG.asp?id=52546 (Mar. 6, 2004).

[61] Shoppers could simply walk out of a store with RFID-tagged products. Readers at the exit would note the items taken, as well as the number of the customer's RFID-enabled loyalty or payment card, and record the proper charge. Receiptless returns would be possible because items would be uniquely tagged and transactions would be recorded. *See* Josh McHugh, *Attention, Shoppers: You Can Now Speed Straight Through Checkout Lines!*, WIRED, July 2004, at 150, *available at* http://www.wired.com/wired/archive/12.07/shoppers.html.

[62] VERISIGN, *supra* note 56, at 4.

known as the Electronic Product Code (EPC), is being developed by a coalition of industry heavyweights, and some predict it will in fact replace the UPC.[63]

EPCs are essentially the wireless version of the UPCs found on barcodes, but with one important exception: EPCs can identify products uniquely at the item level.

> The EPC is a virtual unique license plate for a product that identifies the manufacturer (e.g. Gillette), product class (e.g. Mach 3 Razor), and serial number (e.g. the 574,896th instance of the Mach 3 Razor). Using this EPC, members of the supply chain can thus identify and locate information about the manufacturer, product class, and instance of a particular product. Depending on the type of tag, EPCs can be used to uniquely identify up to 268 million unique manufacturers, each with 16 million types of products. Each unique product can include up to 68 billion individual items, meaning the format can be used to identify hundreds of trillions of unique items.[64]

This range is made possible by the storage capacity available on RFID chips. While UPC barcodes can only store 7 bits of information, EPC RFID tags can store up to 256 bits.[65]

EPCglobal is the standards-setting body that controls the EPC standard.[66] It also controls the network that will make the sharing of EPC information possible.[67] This network includes a naming service, which assigns EPC numbers to manufacturers, as well as a repository of

[63] Mark Baard, *Radio Tag Debut Set for This Week*, WIRED NEWS, *at* http://www.wired.com/news/privacy/0,1848,60408,00.html (Sep. 15, 2003).

[64] VERISIGN, *supra* note 56, at 2.

[65] Steve Meloan, *Toward a Global "Internet of Things,"* SUN MICROSYSTEMS, *at* http://java.sun.com/developer/technicalArticles/Ecommerce/rfid/ (Nov. 11, 2003).

[66] The work to create a standard product code for use with RFIDs began in 1999 at the Auto-ID Center, an academic research group sponsored by industry and headquartered at M.I.T. Once the EPC standard, and the naming and tracking network it powers, were largely perfected, the move to commercialize them through established standards-setting bodies began. In October, 2003, the Auto-ID Center ceased to exist a new standards body, EPCglobal, was created under the auspices of EAN and the UCC. *See generally* EPGGLOBAL, FREQUENTLY ASKED QUESTIONS ABOUT EPCGLOBAL, *at* http://www.epcglobalinc.org/about/faqs.html (last visited Oct. 13, 2004).

[67] VERISIGN, *supra* note 56, at 2

manufacturer-assigned EPC data.[68] The goal of the network is to have complete real-time supply chain visibility, so that manufacturers, retailers, and middlemen have better control over the distribution channels they manage.[69] VeriSign, operator of the World Wide Web top level domains ".com" and ".net," was chosen by EPCglobal to provide the root name system for the EPC Network, which will be based on the Internet's Domain Name System.[70]

2. Government Applications of RFID

Government has also recognized the potential of RFID. Underscoring the notion that the technology's core application is inventory control, the most important government use of RFID to date is asset management by the Pentagon. The military has spent about $100 million over the last decade implementing RFID technology to track everything from rations to uniforms to tanks.[71] The goal is to prevent frontline troops from suffering supply shortages, as well as reducing the amount of lost, misplaced, and unused supplies.[72] Unlike industry, the military has so far focused on active RFID tags—with a price tag of about $100 each—to track vehicles,

[68] For a detailed explanation of how the EPC Network works, *see* VERISIGN, THE EPC NETWORK: ENHANCING THE SUPPLY CHAIN (2004), *available at* http://www.verisign.com/static/002109.pdf. *See also* EPCGLOBAL, ABOUT THE EPCGLOBAL NETWORK, *at* http://www.epcglobalinc.org/about/about_epc_network.html (last visited Oct. 13, 2004).

[69] VERISIGN, *supra* note 56, at 4-5.

[70] *Id*. at 6. *See also* WIRED NEWS, *VeriSign to Manage RFID Tags*, *at* http://www.wired.com/news/business/0,1367,61901,00.html (Jan. 13, 2004).

[71] Alorie Gilbert, *RFID goes to war*, C-NET NEWS.COM, *at* http://news.com.com/2008-1006-5176246.html (Mar. 22, 2004). Another estimate puts Department of Defense RFID spending at $272 million. Cathy Booth-Thomas, *The See-It-All Chip*, TIME, Sep. 22, 2003, at A8, *available at* 2003 WL 58582602.

[72] Alorie Gilbert, *RFID goes to war*, C-NET NEWS.COM, *at* http://news.com.com/2008-1006-5176246.html (Mar. 22, 2004). *See also* Harold Kennedy, *Army Trying to Expedite Flow of Supplies to Troops*, NATIONAL DEFENSE MAGAZINE, *at* http://www.nationaldefensemagazine.org/article.cfm?Id=500 (May 2001) ("Logistics is moving from a 'mass model' of dumping huge amounts of supplies into a combat theater to a 'lean, agile delivery system focused on warfighter needs,' James T. Eccleston, assistant deputy undersecretary of defense for supply-chain integration, told the Quartermaster General's Symposium, in Richmond, Va.").

cargo containers, and other large and valuable assets from long distances.[73] However, it plans to increase its use of passive tags soon.[74]

Other government uses are more theoretical. In a recent report, the FDA endorsed RFID tags as a means to reduce drug counterfeiting, and urged pharmaceutical companies to adopt the technology.[75] Because an RFID network could trace the path a drug takes from its manufacture to its disbursement, it could help verify its authenticity.[76] Meanwhile, the International Civil Aviation Organization (ICAO), the international body responsible for passport standards, recently endorsed the use of RFID on passports.[77] This move has conjured the specter of RFID-equipped driver's licenses or national ID cards.[78] Another rumored government use is placing RFID in currency. According to press reports, the European Central Bank is experimenting with RFID chips in euro notes.[79]

[73] Mark Hachman, *DOD Details its RFID Plans*, EWEEK, *at* http://www.eweek.com/article2/0,1759,1490299,00.asp (Oct. 29, 2003). *See also* Gilbert, *supra* note 71.

[74] *Id*.

[75] FOOD AND DRUG ADMINISTRATION, COMBATING COUNTERFEIT DRUGS 11-13 (Feb. 18, 2004), *available at* http://www.fda.gov/oc/initiatives/counterfeit/report02_04.pdf.

[76] Alorie Gilbert, *FDA endorses ID tags for drugmakers*, C-NET NEWS.COM, *at* http://news.com.com/2100-1008-5161220.html (Feb. 18, 2004).

[77] INTERNATIONAL CIVIL AVIATION ORGANIZATION, FACILITATION (FAL) DIVISION – TWELFTH SESSION REPORT (Apr. 22, 2004), *available at* http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp029_en.pdf.

[78] Ryan Singel, *Passport Safety, Privacy Face Off*, WIRED NEWS, *at* http://www.wired.com/news/privacy/0,1848,62876,00.html (Mar. 31, 2004).

[79] Janis Mara, *Euro Scheme Makes Money Talk*, WIRED NEWS, *at* http://www.wired.com/news/privacy/0,1848,59565,00.html?tw=wn_story_related (July 9, 2003). The reports of RFID in European currency remain speculative, and an Internet rumor that new US $20 bills contained RFID has been dispelled as a hoax (see http://slashdot.org/comments.pl?sid=98942&cid=8437731 and http://www.aimglobal.org/members/news/templates/industry.asp?articleid=106&zoneid=5).

C. The Mandates

Although the UPC standard for barcodes was set in 1973, its use did not catch on until about a decade later.[80] While only 15,000 suppliers were using barcodes in 1984, in three short years that number skyrocketed to 75,000.[81] What happened in 1984?

Wal-Mart's UPC mandate is what happened. Striving as ever to improve its warehousing and distribution, the retail behemoth mandated that any supplier who wanted its business had to use the new barcode on its products.[82] Manufacturers, dependent on the business of the world's largest retailer, obeyed, and today the UPC is ubiquitous. It should be no surprise then that when Wal-Mart announced in mid-2003 that it expected its top 100 suppliers to begin using RFID by January 1, 2005, it effectively launched the RFID revolution.[83]

Not to be outdone, the Department of Defense announced its own RFID mandate, also with a deadline of January 1, 2005.[84] That mandate requires that all of the Pentagon's 46,000 suppliers embed passive RFID chips in each individual product if possible, or otherwise at the level of cases or pallets.[85] While Wal-Mart's eventual goal may be item-level tagging, its initial mandate is only on the case and pallet level.[86]

[80] Granneman, *supra* note 16.

[81] *Id*.

[82] *Id*.

[83] Baard, *supra* note 55. Wal-Mart's other 12,000 suppliers will have until 2006 to comply. *Id.*

[84] Matthew Broersma, *Defense Department Drafts RFID Policy*, C-NET NEWS.COM, *at* http://news.com.com/2100-1008-5097050.html (Oct. 24, 2003).

[85] *Id*.

[86] Eric Peters, *The Watershed Moment for RFID*, C-NET NEWS.COM, *at* http://news.com.com/2010-1071-5072343.html (Sept. 7, 2003).

II. THE PRIVACY CONCERNS OVER RFID

Despite the promise of RFID, many activists have been vocally concerned about the privacy implications of the technology. The ability to track objects is the ability to track persons, they say.[87] In this section, we will see why such fears are overstated. We will also see why the truly worrisome potential uses of RFID are by government, and not by industry where the activists have focused their attention.

A. The Concerns: Some Discerning, Some Daft

In November 2003, a coalition of thirty-five organizations, including the ACLU, EFF, and EPIC, released a position paper on RFID ("Joint Statement").[88] That statement has become one of the most cited articulations of RFID critics' concerns. Specifically, the statement addresses five aspects of the technology that the authors feel could threaten individual privacy.[89]

First, given how tiny RFID tags can potentially be, the ability to hide them in objects and documents without the knowledge of persons later obtaining those items concerns the statement's authors.[90] Second, and related to the first concern, is the ability to hide RFID readers.[91] Third, RFID allows unique numbering of individual items.[92] Fourth, they note that deployment of RFID (as currently envisioned by EPCglobal) "requires the creation of massive

[87] Howard Wolinsky, *Chipping Away at Your Privacy*, CHICAGO SUN-TIMES, Nov. 9, 2003, at 35 ("Tagging individual items '*only* becomes helpful if you want to register individual items to individuals,' said [Katherine] Albrecht, who heads the New Hampshire-based privacy rights group CASPIAN.") (emphasis added).

[88] ALBRECHT ET AL., RFID POSITION STATEMENT OF CONSUMER PRIVACY AND CIVIL LIBERTIES ORGANIZATIONS, *at* http://www.privacyrights.org/ar/RFIDposition.htm (Nov. 2003) [hereinafter Joint Statement].

[89] *Id*.

[90] *Id*.

[91] *Id*.

[92] *Id*.

databases containing unique tag data."[93] They are concerned that such a database could be combined with personally identifying data, essentially linking people to objects.[94] Last, they are concerned that persons may be tracked or profiled without their consent.[95] As an example, they posit a person who has been associated with a shoe being identified by the EPC on that shoe when she attends a political rally.[96] These concerns are echoed in the writings of other critics.[97]

Other less-realistic concerns include the fear that technologically perceptive burglars could case homes by covertly cataloging their contents from the street.[98] More ominously, some critics say "RFID systems could also pose a fatal threat if stalkers manage to adapt the technology to monitor a victim's belongings, embedded with RFID microchips, and track their whereabouts."[99] Perhaps scarier still to some is the possibility that RFID technology could be used for targeted marketing:

> [The potential pervasiveness of tagged products] raises the disquieting possibility of being tracked though our personal possessions. Imagine: The Gap links your sweater's RFID tag with the credit card you used to buy it and recognizes you by name when you return. Grocery stores flash ads on wall-sized screens based on your spending patterns, just like in "Minority Report."[100]

[93] *Id*.

[94] *Id*.

[95] *Id*.

[96] *Id*.

[97] *See generally* Katherine Albrecht, *Supermarket Cards: The Tip of the Retail Surveillance Iceberg*, 79 DENV. U. L. REV. 534, 560-62 (2002) (discussing the use of RFID technology by supermarkets in their marketing programs); Harry A. Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, 2004 STAN. TECH. L. REV. 2, ¶ 92-94 (2004) (noting that RFID systems could "gather unprecedented amounts of individual purchasing habits, and link it to detailed customer information databases").

[98] Valetk, *supra* note 98, at ¶ 93; Declan McCullagh, *RFID Tags: Big Brother in Small Packages*, C-NET NEWS.COM, *at* http://news.com.com/2010-1069_3-980325.html (Jan. 13, 2003).

[99] Valetk, *supra* note 98, at ¶ 93.

[100] Declan McCullagh, *RFID Tags: Big Brother in Small Packages*, C-NET NEWS.COM, *at* http://news.com.com/2010-1069_3-980325.html (Jan. 13, 2003). Other commentators have also mentioned the

Putting aside for the moment the fact that ubiquitous product tagging and pervasive readers, as well as the object databases implicit in the just-mentioned scenarios, are many years away, if indeed they ever materialize, these "disquieting possibilities" may still not be as worrisome as they seem.

1. Concern Over the Concerns: The Daft

One reason why some privacy activist's concerns are unfounded is that today, retailers already track people's purchases to better market to them. The most obvious example is Amazon.com, which welcomes you by name when you visit their Web site, and makes eerily acute recommendations based on your past purchases. In the physical world, supermarkets and other retailers issue customer loyalty cards that help them track consumer spending patterns in order to better stock stores and price products. Checkout receipts now often include coupons targeted to the consumer based on her past purchases.

A "Minority Report" type scenario using RFID, in which a retailer identifies you based on the clothes you are wearing and markets to you by name, is unlikely to occur for two reasons. First, it is very creepy. Such tactics are more likely to alienate customers than impress them; retailers recognize this and will avoid the practice. Second, such a scheme would not be very practical. Identifying an object is not the same thing as identifying a person. A sweater might be bought as a gift, lent out, or sold secondhand on eBay. Retailers will not risk embarrassment by making assumptions about identity.[101]

"Minority Report" scenario. *See* Elisa Batista, *What Your Clothes Say About You*, WIRED NEWS, *at* http://www.wired.com/news/wireless/0,1382,58006,00.html (Mar. 12, 2003).

[101] But notice that a substitute for the person-identifying retina-scan in "Minority Report" would be a government-mandated RFID ID card. Unlike a book you purchased, the odds are very good that only you carry your driver's license. *See generally* Jay Stanley & Barry Steinhardt, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, (ACLU/Technology and Liberty Program Jan. 2003), at 5, 13, *at* http://www.aclu.org/Privacy/Privacy.cfm?ID=11573&c=39 (discussing how RFID could be combined with a

Similarly, while some worry that burglars will equip themselves with $500 RFID readers to "drive by a home and say, 'Look what we've got in there. An HDTV is in there, and she wears Benetton,'"[102] the fact is that burglars today already case homes by such low-tech means as looking through windows. Furthermore, the technical limitations of RFID might not make such casing very feasible. The range of RFID tags in the EPC standard is twenty to thirty feet at most.[103] The Inverse Square Law of physics prescribes that the further one is from the tag, the more energy a reader will have to employ to read it.[104] This makes long-range readers hardly portable or easily powered. Also, RF signals cannot pass through metal, liquids, and other dense materials, making long-range reading even more difficult.[105] Finally, if you are still worried that a burglar will be able to read the contents of your home, you can install an RFID blocker device.[106]

Many of the fears about RFID stem from a misunderstanding of the technology. One commentator fretted that "RFID systems would expose consumers to needless risk by allowing

national ID card for tracking and access control purposes). Government tracking by means of mandatory national ID cards is further discussed in section II.C, *infra*.

[102] Elisa Batista, *What Your Clothes Say About You*, WIRED NEWS, *at* http://www.wired.com/news/wireless/0,1382,58006,00.html (Mar. 12, 2003).

[103] Collins, *Alien Upgrades Its EPC Reader*, RFID JOURNAL, *at* http://www.rfidjournal.com/article/articleview/825/1/ (Mar. 11, 2004). Also, retailers will not use tags that are any more powerful than necessary for their purposes given that a tag's read-range and frequency correlates to its price.

[104] *See* Steven Blusk, *Tutorial: Measuring Time & Distance*, *at* http://physics.syr.edu/courses/CCD_NEW/seti/tutorial/measure/part6.html (last visited Oct. 9, 2004).

[105] Finkenzeller, *supra* note 1, at 141-42; Mark Baard, *Is RFID Technology Easy to Foil?*, WIRED NEWS, *at* http://www.wired.com/news/privacy/0,1848,61264,00.html (Nov. 18, 2003).

[106] *See generally* Matt Hines, *RSA Polishes RFID Shield*, C-NET NEWS.COM, at http://news.com/2100-1029-5164014.html (Feb. 24, 2004) (discussing a jamming system that confuses RFID readers outside certain boundaries); Ari Juels & John Brainard, *Soft Blocking: Flexible Blocker Tags on the Cheap*, (RSA Laboratories Apr. 2004), *at* http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/softblocker/softblocker.pdf (proposing a cheaper and more flexible variant of blocker technology that allows partial reading instead of the all-or-nothing approach of ordinary blockers).

tech-savvy burglars to inventory a victim's house from a distance,"[107] and proceeded to cite to a news story about Wi-Fi wardriving.[108] RFID is not Wi-Fi (nor is it GPS as we will see below).[109] Another commentator seemed to grasp the limitations, but nevertheless cast the threat like so: "Future burglars could canvass alleys with RFID detectors, looking for RFID tags on discarded packaging that indicates expensive electronic gear is nearby."[110] But burglars today do not need RFID readers to spot the plasma screen TV crate on your curbside.

Even if criminals or overzealous marketers could put the technology to use for nefarious purposes, it should not be proscribed, as some would have it.[111] Doing so would be like limiting telephone technology because ransom demands or telemarketing messages could be communicated across the wires.[112] Criminal activity is unlawful, whether it involves RFID technology or not. How retailers and marketers may use information they collect about consumer habits is a debate that existed before RFID, and that debate is independent of the technology employed by marketers. The fact that a debate exists should no more affect the adoption of RFID technology than it should ban Web cookies or existing loyalty programs.

[107] Valetk, *supra* note 99, at ¶ 93.

[108] Xeni Jardin, *Wireless Hunters on the Prowl*, WIRED NEWS, *at* http://www.wired.com/news/wireless/0,1382,59460,00.html (July 2, 2003). Wardriving is the practice of driving around in a car with a Wi-Fi-equipped laptop in search of unprotected networks and open hotspots.

[109] Unlike RFID tags, Wi-Fi base stations have large antennas and ample power to transmit their signals far and wide. Indeed, the purpose of Wi-Fi transmitted is to exchange large amounts of data throughout buildings and large areas. This is in contrast to the limited capacity of RFID tags.

[110] McCullagh, *supra* note 101.

[111] Hiawatha Bray, *Usefulness of RFID Worth the Annoyance*, BOSTON GLOBE, Apr. 12, 2004, at D2 (quoting RFID privacy activist Katherine Albrecht: "I think the main way we're going to prevent RFID abuse is to limit its implementation.").

[112] *Id*. ("Albrecht's a smart and charming woman, but she might have opposed the invention of the telephone, out of fear that the government would listen in. She'd have been right, too. But we dealt with that problem through laws, not by abandoning the idea of telecommunications.")

These daft concerns overstate the threat of RFID because they do not take into account the limitations of the technology or the self-interest of retailers. It is the more legitimate concerns of privacy activists, embodied in the Joint Statement, which should be more carefully addressed.

2. Concern Over the Concerns: The Discerning

The five points of the Joint Statement can be summed up this way: RFID will allow individual persons to be tracked (1) at all times, (2) without their knowledge or consent. These are serious concerns. But, as we will see, there is less cause for alarm than such a statement might seem to suggest.

The idea that one can be tracked anywhere and at any time conjures up the image, often seen in the movies, of a blip on a screen representing a person and her every move. Her pursuer, privy to this information, need only overtake her at the next corner. No wonder some are concerned about stalkers using RFID against their victims to "track their whereabouts."[113] But this concern seems to conflate RFID with GPS, or simply with the idea that the location of a "bugged" person can be pinpointed at will.[114]

GPS can be used to locate a lost hiker or a stolen car because a GPS device can not only use the information from satellites orbiting the earth to locate its exact position, but might also contain a high-powered radio transmitter (not unlike that of a cell phone) that broadcasts its location. But tiny RFID tags cannot read satellite signals, nor do they transmit strong radio

[113] Valetk, *supra* note 99, at ¶ 93.

[114] Katherine Albrecht, *Supermarket Cards: The Tip of the Retail Surveillance Iceberg*, 79 DENV. U. L. REV. 534 at 561 (2002) ("[EPC Network technology] would allow for seamless, continuous identification and tracking of physical items as they move from one place to another, enabling companies to determine the whereabouts of all their products at all times."); Electronic Frontier Foundation, EFF: Radio Frequency Identification (RFID), at http://www.eff.org/Privacy/Surveillance/RFID/ (last visited July 7, 2004) ("[RFID is] a technology that pinpoints the physical location of whatever item the tags are embedded in. While this seems like a convenient way to track items, it's also a convenient way to do something less benign: track people and their activities through their belongings.")

signals, especially without a prompt from a reader. A better analogy for how RFID tags help "track" an item is the way a barcode helps FedEx "track" a package.[115]

The process of sending a letter via FedEx begins when you seal and address the letter and take it to your nearest drop-off point. The FedEx label you affixed to the package has a unique identification number and a corresponding barcode—for your records, you keep a copy of that number. A FedEx employee scans the barcode and enters the destination of the letter into the computer. The unique number is associated with your letter's destination in FedEx's database.

The employee places the letter in the appropriate bin or conveyor belt and off it goes on its journey. When the letter leaves the building, its barcode is scanned, and a notation is made in the database: "Left Washington, DC on 4/15/04 at 5:39 p.m." When it gets to the airport it is scanned again and another notation is made: "Arrived Dulles Airport on 4/15/04 at 7:45 p.m." The letter is scanned each step of the way: on the plane, at the other airport, at the sorting facility, on the truck, and finally with a hand-held scanner when its delivery is confirmed.

At any time after drop-off you can log on to FedEx's Web site, enter the letter's unique number, and see the location where it was last scanned. In this sense you can "track" your package, but this does not mean you know where it is at any given moment. The database might say, "On the plane to Bangkok," but your package might well be on the ocean floor. Your information is only as good as the last place where the letter's RFID tag was read. In this same way, RFID tags will allow manufacturers, distributors, and retailers to track items throughout the supply chain, but it will not let them know where an item is at any given moment.

[115] In fact, shipping companies like FedEx are looking at replacing or complementing barcodes with RFID. Kristen Philipkoski, *FedEx Delivers New Tech Lab*, WIRED NEWS, *at* http://www.wired.com/news/business/0,1367,61266,00.html (Nov. 19, 2004).

To track you in any meaningful way, a stalker would have to have access to the databases of the retailers from which you have purchased RFID-tagged items (that you may or may not have in your possession at the moment) in order to know which EPC numbers correspond to you. (And this, of course, assumes that retailers will link personally identifying information to EPC numbers and keep this information in a database.) Once she has those numbers, the stalker will need to have a network of RFID readers throughout the geographic area she wishes to search. Even then, your stalker will only know that an item linked to your name was scanned at a certain place at a certain time. If you have lent or sold or even thrown away any of your items, she might find that you are in five different places at once. There are better ways for stalkers to follow persons; EPC tags will not put anyone's life at risk.

Nor is RFID practical to discover which persons attended a political rally, as the Joint Statement authors and others fear.[116] First, assuming that there is a database linking you to every RFID-tagged consumer product you have ever purchased at any and all retailers, the presence of an item linked to you at a political rally may well still be a false positive, as explained above. Second, how would the persons interested scan the crowd at a rally? Given the read-ranges of RFID tags, they would either have to make sure everyone passed through a reader-equipped gate of some sort, or they would have to inconspicuously get near enough to each person to scan them. They would also have to contend with reader detectors and jammers.[117]

[116] Joint Statement, *supra* note 88; Alan Cohen, *No Where* [sic] *To Hide*, PC MAGAZINE, *at* http://www.pcmag.com/article2/0,1759,1612820,00.asp (July 13, 2004) ("Your sweater could then become a sort of homing beacon. Install enough readers and it wouldn't seem too hard to note every political rally you've attended….").

[117] *See supra* note 106. Unwanted RF transmissions have already met blocking technology. Cell phones have been jammed to prevent their ringing, especially at movie theatres and concert halls. Sam Lubell, *Block That Ring Tone!*, N.Y. TIMES, Apr. 8, 2004, at G1.

It would therefore seem that a more traditional means of discovering who attends a rally, such as photo or video surveillance, would be more efficient. This, again, raises the issue of hating the game, not the player.[118] That is, there exists an ongoing debate over the propriety of public surveillance,[119] but that debate is independent of the technology employed. The fact that an unresolved debate exists, and that RFID might possibly be used for surveillance, should not limit the technology's adoption in areas where there is no doubt it will be appropriate and useful. More to the point, what motivation would retailers have to identify persons at a political rally? To target-market "Future Dem" baby bibs? More likely, who we fear will use this technology to keep an eye on rallies is the government, much as it has done for years.[120] But if this is the case, it simply means that there is another game to hate, whoever the player, as we will see in Section II.C below.

Related to the fear that one will be tracked anywhere, critics are concerned that RFID will be used to track individuals in their own homes.[121] This brings us to the second aspect of the Joint Statement's concern, that persons will be tracked without their knowledge or consent. In

[118] Ice-T, *Don't Hate the Playa, on* 7TH DEADLY SIN (Atomic Pop 1999).

[119] For differing conceptions of privacy and privacy protection, *see generally*, Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125 (2000); Richard Posner, *An Economic Theory of Privacy*, REGULATION, May-June 1978, at 19.

[120] *See generally* Natsu Taylor Saito, *Whose Liberty? Whose Security? The USA PATRIOT Act in the Context of COINTELPRO and the Unlawful Repression of Political Dissent*, 81 Or. L. Rev. 1051(2002) (discussing the history of government surveillance of political activity, including the FBI's "counter-intelligence program" of the 1960s and 1970s aimed at anti-war and civil rights activists); Peter Slevin, *Police Cameras Taped Football Fans*, WASH. POST, Feb. 1, 2001, at A01 (discussing government surveillance of fans with the use of face recognition technology at Super Bowl XXXV).

[121] Katherine Albrecht, *Supermarket Cards: The Tip of the Retail Surveillance Iceberg*, 79 DENV. U. L. REV. 534 at 562 (2002) ("As incredible as it may seem, [marketers] are now planning ways to monitor consumers' use of products within their very homes. Auto-ID tags coupled with indoor receivers installed in shelves, floors, and doorways, could provide a degree of omniscience about consumer behavior that staggers the imagination."); Jonathan Krim, *Embedding Their Hopes In RFID*, WASH. POST, June 23, 2004, at E01 ("[Katherine Albrecht] worries that companies putting tags into consumer products might forge alliances with the makers of carpeting, for example, to embed sensing devices that could develop intelligence about how consumers use the items.").

particular, critics fear that retailers will use credit card numbers to link individuals to their purchases. But it is interesting to note that while this is feasible today, consumers continue to opt for loyalty programs. There are good reasons for this.

Consumers would likely not look kindly on anyone but their credit card company keeping a list of their credit card numbers without their permission. Retailers are happy to avoid the market backlash that doing so might bring. They are also happy to avoid the potential liability that might result if only a few of the collected credit card numbers are mishandled.[122] Today, any sensible merchant knows not to keep on file the credit card information of its customers because nothing good can come from doing so. Additionally, credit card companies do not want their customers' credit card numbers stored or used as identifiers by retailers and will make this part of merchant agreements as they do today.[123]

This de facto privacy protection policy further underscores the fact that the theoretical privacy debate should be separated from the technology. Whether retailers should be able to use your credit card information in combination with a database to track purchases is a question that has nothing to do with item-level tagging of consumer goods using RFID.

Joining a loyalty program is a choice consumers make.[124] If retailers do not abide by their program's agreement, they are liable for breach. Similarly, retailers value the business of customers who choose not to participate and will not want to invite their ire by tracking them

[122] *See* Jonathan Krim, *Insider Case At AOL Shows Vulnerability*, WASH. POST, June 26, 2004, at E01 (describing how an America Online software engineer stole a list of e-mail addresses for the company's 92 million subscribers and then sold it to spammers.).

[123] *See, e.g.*, FINDLAW, *Merchant Agreement - Electronic Payment Exchange Inc., Certegy Card Services Inc., First Union National Bank and PayPal Inc.*, *at* http://contracts.corporate.findlaw.com/agreements/paypal/certegy.merchant.2001.11.14.html (last visited Sept. 10, 2004). Sample credit card merchant agreement including terms on the use of customer data. *Id.* §§ 20(o) - (q), 21, and 30.

[124] Some critics say consumers do not have a choice in the matter, but that is a debate over market power and is addressable by antitrust regulations, not privacy laws.

nonetheless. Companies have begun to publish EPC privacy statements to which they will also be held accountable.[125] These statements include promises to clearly label the use of RFID tags and make them easily removable.[126] Regulation of RFID is unnecessary unless we find that market forces have failed to constrain practices that make us uncomfortable. In fact, regulation may be unnecessary altogether because RFID may never be ready for primetime.

B. The Elephant in the Room: RFID Might Not Work

The promise of RFID might be as over hyped by its proponents as its threats are by its critics. As one technologist put it, "People are a bit focused on its usage potential as opposed to how to make it really happen."[127]

In fact, the push for general adoption of RFID seen today would have likely never happened but for the Wal-Mart mandate.[128] And although Wal-Mart's stamp of legitimacy does give the technology a big boost, it does not mean that it will work.[129] Wal-Mart is not infallible, and if RFID does not work out, the retail giant will have no qualms about dropping the venture.[130]

[125] Procter & Gamble, *P&G Position on Electronic Product Coding (EPC), at* http://www.pg.com/company/our_commitment/privacy_epc/epc_position.jhtml (last visited July 25, 2004); Wal-Mart, *Radio Frequency Identification Usage, at* http://www.walmartstores.com/wmstore/wmstores/Mainsupplier.jsp?catID=-8250&categoryOID=-10605&pagetype=supplier&template=DisplayAllContents.jsp.

[126] *Id*.

[127] Matt Hines, *RFID Revolution: Are We Close?*, C-Net News.com, *at* http://news.com.com/2008-1039-5168489.html (Mar. 3, 2004) (quoting Rainer Kerth, IBM RFID expert).

[128] Matt Hines, *RFID: Is It Soup Yet?*, C-Net News.com, *at* http://news.com.com/2008-1013-5205486.html (May 6, 2004). Indeed, as the failure of the Prada New York store shows, retailers might be foisting RFID technology on consumers before they are ready, and they may reject it. *See supra* note 42.

[129] Erika Morphy, *What RFID Can Do for Consumers*, CRM Daily, *at* http://crm-daily.newsfactor.com/story.xhtml? story_id=24123 (May 20, 2004).

[130] *Id*.

We now know that the overwhelming majority of Wal-Mart's top suppliers will not be able to meet the January 2005 deadline for adopting RFID.[131] Only about 25 percent of suppliers will likely meet the goal—a precipitous drop from a previous estimate of 60 percent.[132] Complying with Wal-Mart's guidelines will cost a typical supplier about $9 million, and up to $100 million in some cases.[133] These outlays come with no immediately apparent return on investment, and most suppliers can only hope to minimize losses from complying with the mandate.[134]

If RFID is ultimately adopted, it will not be for a long while. The cost of tags needs to drop significantly before they can be deployed profitably on product lines.[135] Item-level tagging will not be prevalent until RFID tags cost at most five cents each, and this puts such tagging at least seven years away.[136] Adding to the cost of deploying RFID is the fact that there are very few, if any, consultants with a track record of successful implementations.[137] Hiring expertise is

[131] Matt Hines, *RFID Deadline Hits a Wall, Study Says*, C-NET NEWS.COM, *at* http://news.com.com/2100-1006-5182579.html (March 31, 2004); Christine Spivey Overby, *RFID At What Cost? What Wal-Mart Compliance Really Means*, FORRESTER RESEARCH, *at* http://www.forrester.com/Research/Document/Excerpt/0,7211,33695,00.html.

[132] *Id*.

[133] *Id*.

[134] Larry Dignan & Kim S. Nash, *RFID: Hit or Myth?*, EWEEK, *at* http://www.eweek.com/article2/0,1759,1524634,00.asp (Feb. 9, 2004).

[135] Erika Morphy, *Analysis: The RFID vs. Privacy Debate*, CRM DAILY, *at* http://crm-daily.newsfactor.com/story.xhtml? story_id=23289 (March 3, 2004);

> Retailers and CPG manufacturers bought into the idea that they could use RFID tags economically if they cost €0.05. But complex manufacturing techniques, a costly assembly process, and a lack of demand means the price of RFID tags won't drop to €0.05 in the next eight years. The Forrester model forecasts that RFID tag prices will decline, on average, only 9% year on year.

Charles Homs, *Exposing The Myth Of The 5-Cent RFID Tag*, FORRESTER RESEARCH, *at* http://www.forrester.com/Research/Document/Excerpt/0,7211,33905,00.html (Feb. 23, 2004).

[136] *Id*.

[137] *Id*.

very expensive.[138] There is also little motivation to adopt RFID immediately since UPC barcodes work fine today.[139] Given that there is a vast installed base of legacy barcode systems, there will likely be "considerable inertia" in adopting RFID.[140]

Wal-Mart might also be the exception, not the rule. Wholesale distributors have very little incentive to adopt RFID:

> Distributors purchase products from manufacturers at bulk discounts. They assume the market risk, reselling the goods for a profit to retailers. With radio identification, it's possible that these middlemen could be cut out of the process. Manufacturer and retailers would know the balance of supply and demand in real-time and, as a result, could choose to deal directly with each other.[141]

Additionally, the benefits of the EPC Network assume a vast sharing of information among participants in a supply chain to increase visibility. This presumes an unprecedented level of cooperation, and disregards the market for information.[142] "Knowledge is power—if retailers readily disgorge information of interest to manufacturers, they may weaken their negotiating position vis-à-vis their suppliers," one observer has noted.[143] "And, to the degree that retailers are able to interrogate RFID-bearing items on their shelves, other parties, to include competitors, may be able to do so as well."[144]

If the business disincentives to adoption do not convince you that RFID's prospects are not as rosy as some would suggest, there are always the technology's technical limitations. As

[138] Jo Best, *RFID: Too Few Experts, To Dear and Tech Not Good Enough*, SILICON.COM, *at* http://management.silicon.com/itdirector/0,39024673,39119783,00.htm (April 5, 2004).

[139] ROSS STAPLETON-GRAY, SCANNING THE HORIZON: A SKEPTICAL VIEW OF RFIDS ON THE SHELVES 2 (Nov. 13, 2003), *at* http://www.stapleton-gray.com/papers/sk-20031113.pdf.

[140] *Id*. at 2.

[141] Dignan & Nash, *supra* note 134.

[142] STAPLETON-GRAY, *supra* note 139, at 5.

[143] *Id*.

[144] *Id*.

mentioned above, the signals emitted by RFID tags cannot penetrate metal, liquids, and other dense materials.[145] Even things like cold storage, humidity, and microwaveable containers hurt reliability.[146]

Barcodes are 99 percent accurate.[147] Without at least the same reliability, RFID is all but useless. Field tests carried out by the Auto-ID Center to simulate real-world distribution scenarios returned disappointing results. Only 78 percent of tags were read during the four-month trial.[148] While a relatively friendly environment like a distribution center could be engineered to minimize interference, a retail store floor with RFID tags scattered throughout is a comparatively hostile setting.[149] Self-service checkout also requires near 100 percent reliability, and so "is likely to be a pipedream."[150] Even Wal-Mart acknowledges that such a check-out system is at least ten to fifteen years away.[151]

Finally, while barcodes are easily standardized across the world, RFID standardization is more difficult because it is dependent on the radio spectrum, which is regulated differently by each country's government.[152] It therefore seems that RFID-tagging of consumer products is confronted with more obstacles than either its critics or proponents care to admit.

[145] Finkenzeller, *supra* note 1, at 141-42; Mark Baard, *Is RFID Technology Easy to Foil?*, WIRED NEWS, *at* http://www.wired.com/news/privacy/0,1848,61264,00.html (Nov. 18, 2003).

[146] Dignan & Nash, *supra* note 134.

[147] *Id*.

[148] *Auto-ID Center Field Test Report*, RFIDJOUNRAL.COM *at* http://www.rfidjournal.com/article/articleview/84/1/1/ (Oct. 4, 2002).

[149] STAPLETON-GRAY, *supra* note 139, at 3.

[150] *Id*.

[151] Dignan & Nash, *supra* note 134.

[152] *Spectrum Needs, Privacy Issues Debated for RFID Technologies, COMMUNICATIONS DAILY,* Apr. 2, 2004, *available at* 2004 WL 60705576. *See also* Hines, *supra* note 127.

C. The Real Threat to Privacy Is From Government

The nightmare scenario of RFID critics is the tracking of persons—either at a political rally, by a stalker, or by a retailer who wants to engage in targeted marketing. But as we saw above, the use of EPC numbers to track individuals is impractical, if not impossible. For one thing, EPC numbers would only correspond to items, and associating a person to an item would mean hazarding a guess at best. However, one scenario eliminates the guesswork: government assigning a unique number to each individual.

One critic, contemplating the various possibilities of a surveillance state, posited the following scenario:

> A tourist walking through an unfamiliar city happens upon a sex shop. She stops to gaze at several curious items in the store's window before moving along. Unbeknownst to her, the store has set up the newly available "Customer Identification System," which detects a signal being emitted by a computer chip in her driver's license and records her identity and the date, time, and duration of her brief look inside the window. A week later, she gets a solicitation in the mail mentioning her "visit" and embarrassing her in front of her family.[153]

But notice that without a government-mandated chip, which identifies the woman uniquely, this scenario could not take place so easily. Attempting to guess her identity by reading EPC numbers on her clothes, for example, might prove difficult. It would require access to the EPC Network, which a sex shop may not be as likely to have, and it ultimately would only be a guess. But a government ID number identifies the person, not an item. A database that correlates government ID numbers, names, and other personally identifying information could be reverse-engineered, much like the Internet Movie Database was developed without the help of

[153] Jay Stanley & Barry Steinhardt, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, (ACLU/Technology and Liberty Program, New York, N.Y.) Jan. 15, 2003, at 5, at http://www.aclu.org/Privacy/Privacy.cfm?ID=11573&c=39.

industry.[154] The less reputable a retailer is, the more likely they will engage in such "creepy" direct marketing. Similarly, a government ID would pose a much greater threat to anonymity than a consumer product that has been tagged with an EPC number, and this would make a stalker's task a bit easier.

If one is truly concerned about government tracking of individuals at political rallies or anywhere else, then a national ID, especially one equipped with RFID or other Auto-ID technology, should be the focus of one's attention. The involuntary nature of a government mandate makes it particularly dangerous. The recent *Hiibel v. Sixth Judicial District Court of Nevada, Humboldt County*[155] decision found that citizens could not refuse to identify themselves when agents of the state demand it. It may only be a matter of time before government facilitates compulsory identification by mandating a national ID card embedded with RFID chips.

National ID card legislation has been proposed and seriously considered after the terrorist attacks of September 11, 2001.[156] Last year, delegates to the Chinese Communist Party Congress were required to wear an RFID badge at all times so that their movements could be tracked and recorded.[157] Today, passports may soon be equipped with RFID tags,[158] and the Department of Homeland Security is currently developing RFID-enabled IDs to be used at border crossings.[159] The growing campaign by government to require its citizens to identify themselves, regardless of the technology employed, is the greatest threat to anonymity. Yet,

[154] *See* INTERNET MOVIE DATABASE, *IMDb History*, *at* http://www.imdb.com/Help/Oweek/history.html. A fledgling reverse-engineered database of UPC product codes is also available at http://www.upcdatabase.com.

[155] Hiibel v. Sixth Judicial Dist. Court, 72 U.S.L.W. 4509 (U.S. June 21, 2004).

[156] Steven Levy, *Playing the ID Card*, NEWSWEEK, May 13, 2002, *available at* 2002 WL 7294218.

[157] Granneman, *supra* note 16.

[158] ICAO, *supra* note 77.

[159] Jonathan Krim, *U.S. May Use New ID Cards At Borders*, WASH. POST, June 5, 2004, at E01.

critics of RFID continue to focus on private uses of the technology, and mention threats from government only in passing.[160]

III. THE FOLLY OF RFID LEGISLATION

In March 2004, Senator Patrick Leahy (D-VT.) became the most prominent politician to address the privacy concerns over RFID. He did so with a speech before a privacy and security conference at Georgetown University Law Center. Calling RFID tags "barcodes on steroids," he said that while there may be many business advantages to using them, "RFIDs seem poised to become the catalyst that will launch the age of micro-monitoring."[161]

"[T]he RFID train is beginning to leave the station," he warned, "and now is the right time to begin a national discussion about where, if at all, any lines will be drawn to protect privacy rights."[162] Leahy called for congressional hearings before the "RFID genie is let fully out of its bottle."[163] Such a dialogue, if truly open-minded, can indeed be very helpful in educating everyone involved about the possibilities and limits of RFID, as well as about the legitimate concerns of the privacy sensitive public.

The Joint Statement similarly calls for such a debate. It asks industry to impose a voluntary moratorium on item-level tagging until a "formal technology assessment" sponsored

[160] Both the Joint Statement and proposed privacy guidelines put forth by EPIC focus on private uses of RFID, and mention government use only in passing. This is representative of how most privacy advocates have approached the issue. Joint Statement, *supra* note 88 ("Although not examined in this position paper, we must also grapple with the civil liberties implications of governmental adoption of RFID."); ELECTRONIC PRIVACY INFORMATION CENTER (EPIC), *Proposed Guidelines For Use of RFID Technology: Enumerating the Rights and Duties of Consumers and Private Enterprises*, *at* http://www.epic.org/privacy/RFID/rfid_gdlnes-062104.pdf (June 21, 2004) ("[T]hese guidelines do not address protection of consumer privacy from any governmental action. Rather these guidelines seek to protect consumer privacy form private enterprises.").

[161] Senator Patrick Leahy, Address at the Georgetown Law Center conference on "Video Surveillance: Legal and Technical Challenges" (Mar. 23, 2004), *at* http://leahy.senate.gov/press/200403/032304.html.

[162] *Id*.

[163] *Id*.

by a "neutral entity" is completed.[164] However, there are some points the Joint Statement deems non-negotiable, and it lists several "RFID practices that should be flatly prohibited."[165] The Federal Trade Commission recently took a first step toward a national dialogue by hosting a one-day conference on RFID at which all sides of the debate gathered to participate.[166]

But despite calls for reasoned reflection, and despite how much time there is before RFID is ever seriously implemented, some still wish to nip this technology in the bud. They refuse to separate the technology from the larger privacy debate, and they will not wait to see if market and cultural forces can acceptably shape RFID practices on their own.[167] Katherine Albrecht, head of Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), the group that has taken the lead opposing RFID, stated it succinctly when she said, "I think the main way we're going to prevent RFID abuse is to limit its implementation."[168] Boycotts and protests by CASPIAN have caused Italian clothier Benetton and German supermarket chain Metro to forsake RFID tests.[169] Sadly, the restless desire to forgo a national dialogue, and deal a blow to RFID today, is shared by lawmakers in several states.

[164] Joint Statement, *supra* note 88.

[165] *Id*. By necessity, "flatly prohibited" means legal restraints.

[166] *See* FEDERAL TRADE COMMISSION, R*adio Frequency IDentification: Applications and Implications for Consumers*, *at* http://www.ftc.gov/bcp/workshops/rfid/ (last visited July 11, 2004).

[167] An example of the market disciplining the use of technology is the failure of the New York Prada store discussed above. *Supra* note 42. *See also* Ben Woodhead & Emma Connors, *Chips out of fashion at Prada*, AUSTRALIAN FINANCIAL REVIEW, *at* http://www.afr.com/articles/2003/10/20/1066631355534.html (Oct. 21, 2003) ("'It turns out the ladies who shopped at Prada objected to the data collected [using RFID loyalty cards],' said Terry Retter, a technology forecaster at PriceWaterhouseCoopers. 'They didn't mind Prada keeping track of what they bought and when, but they did mind the store knowing what size they wore.'")

[168] Bray, *supra* note 111.

[169] Elisa Batista, *'Step Back' for Wireless ID Tech?*, WIRED NEWS, *at* http://www.wired.com/news/wireless/0,1382,58385,00.html (Apr. 8, 2003); Kim Zetter, *Germans Protest Radio-ID Plans*, WIRED NEWS, *at* http://www.wired.com/news/business/0,1367,62472,00.html (Feb. 28, 2004).

A. Proposed RFID Legislation

Legislators in California, Utah, and Missouri have introduced bills to regulate RFID, and at least one legislator in Massachusetts says he will follow suit.[170] While the Missouri bill would only require retailers who sell RFID-tagged products to label this fact conspicuously,[171] the California and Utah bills go further. The Utah bill not only requires notice to consumers about the presence of RFID, it requires manufacturers and distributors to alert retailers of the presence of tags and teach them how to kill the tags if possible.[172] It also provides a private right of action to enforce the provisions of the bill.[173] The Utah bill is based on a federal "RFID Right to Know Act" proposed by CASPIAN, which would amend several portions of the U.S. Code.[174]

The California bill,[175] though heavily amended from its original version, is the most far-reaching. It prohibits item-level tagging that "*enables* the user" to collect information from tags that "*could* be used to" identify individuals unless certain conditions are met.[176] Among the conditions are the following restrictions: (1) Collected information must be provided by the "customer for the purpose of completing a transaction to purchase or rent an item containing an RFID tag at a retail store," and (2) "the information [must not be] collected at any time before a customer actually initiates a transaction to purchase or rent an item or at any time after the

[170] Joanna Ramey, *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.

[171] S.B. 867, 92nd Gen. Assem., 2d Reg. Sess. (Mo. 2004).

[172] H.B. 314, 56th Leg., 2004 Gen. Sess. (Utah 2004).

[173] *Id*.

[174] Mark Baard, *Lawmakers Alarmed by RFID Spying*, WIRED NEWS, *at* http://www.wired.com/news/privacy/0,1848,62433,00.html (Feb. 26, 2004); *See* Zoe Davidson, *RFID Right to Know Act of 2003*, (CASPIAN, Boston, Mass.), *at* http://www.spychips.com/press-releases/right-to-know-bill.html (last visited July 11, 2004).

[175] S.B. 1834, 2003-2004 Reg. Sess. (Cal. 2004).

[176] *Id*.

customer completes the transaction."[177] There is no provision in the bill allowing customers to voluntarily opt-in and consent to use of their information beyond what is provided for in the bill.[178] The bill also specifically places similar restrictions on lending libraries.[179]

Under such a law, it is not clear that an application of RFID similar to the one by Prada in New York would be permissible. The California bill does not seem to allow voluntary use of RFID-enabled loyalty cards that could help retailers give specialized attention to their customers. Even if such a loyalty program were permitted, the California bill only allows the use of RFID "for the purpose of completing" a sale, and restricts the technology's use until "a customer actually initiates a transaction to purchase."[180] This would seem to eliminate the possibility that a customer could take advantage of RFID to shop without actually purchasing. For example, an RFID-enabled store in Germany uses the technology to let customers know where the items they are looking for are located in the store.[181] Additionally, the bill's restriction on collecting information "at any time after the customer completes the transaction"[182] would seem to preclude post-purchase conveniences like receiptless returns.

It is interesting to note that this is an amended version of the bill. The original proposal would have required written consent before any individually identifiable information about a person was attached to data collected via an RFID system, or shared with a third party.[183] The

[177] *Id*.

[178] *Id*.

[179] *Id*.

[180] *Id*.

[181] McHugh, *supra* note 61. The same store also features a video section where holding up a DVD to a screen will play a trailer of the selected movie. *Id*.

[182] S.B. 1834, 2003-2004 Reg. Sess. (Cal. 2004).

[183] S.B. 1834, 2003-2004 Reg. Sess. (Cal. 2004), introduced version dated Feb. 20, 2004.

original bill also required retail stores to detach or destroy RFID tags on consumer products before they left the premises.[184] Other critics have proposed this popular solution as well.[185] But as some have noted, not only would this requirement preclude post-purchase applications of RFID, it also amounts to an unfunded mandate.[186] Not all retailers are Wal-Mart; most are small "mom and pop" stores that will lack the ability to detect, much less kill, RFID tags. Requiring *all* retailers to kill tags embedded by manufacturers in consumer products creates great pressure against use of the tags. Perhaps most interesting to note is that the original version of the California bill placed its restrictions on "persons or entities."[187] The amended bill carefully replaces that phrase with "private entities" and "libraries," thereby leaving government agencies free to use RFID as they please.

B. Legislation Is Unnecessary and Harmful

If the technical limitations and cost of RFID do not prevent its deployment, restrictive legislation just might. Critics and legislators are jumping to conclusions and hating the player instead of the game. Simply because a technology *could* be used in harmful ways does not mean that it will. One needs to look no further than the failure of RFID at Prada's New York store, the impending failure of manufacturers to meet Wal-Mart's mandate, or the RFID policy changes announced by Benetton and Metro to see that market forces constrain businesses. We should not regulate new technologies until we know how they will play out in the market. To do otherwise is to risk killing useful and wealth-creating technologies before they have had a chance to become viable. We would forgo all the unexpected and creative applications that are spawned

[184] *Id*.

[185] ELECTRONIC PRIVACY INFORMATION CENTER (EPIC), *supra* note 164, at 2-3.

[186] STAPLETON-GRAY, *supra* note 139, at 4.

[187] S.B. 1834, 2003-2004 Reg. Sess. (Cal. 2004), introduced version dated Feb. 20, 2004.

once a technology is widely adopted—the Internet, for example, was never meant to be an auction house or a dating service.

It is already becoming apparent how retailers and other companies plan to address the privacy concerns of consumers. (After all, we should not forget that consumers are the persons on whom retailers depend for their continued existence and prosperity.) A recent survey by market analysis firm Forrester Research found that 21 percent of U.S. consumers who are aware of RFID tags fear the prospect of companies tracking their purchases.[188] Forrester suggested that retailers develop an RFID code of conduct to help align their business plans with consumer sentiments.[189] They also suggested that because many consumers would appreciate that tags be killed before they left the store, that retailers consider this as an option.[190] Not surprisingly, industry has taken the hint.

EPCglobal has released a set of guidelines for EPC on consumer products.[191] These include giving clear notice of the presence of RFID on products, as well as the ability to disable or discard RFID tags.[192] Procter & Gamble, one of the largest early adopters of RFID technology, has adopted very similar privacy guidelines.[193] Regulation, and all its attendant costs, is unnecessary unless market forces fail to meet consumer preferences on privacy.

[188] Christine Spivey Overby, *Commentary: An RFID code of conduct*, C-NET NEWS.COM, *at* http://news.com.com/2030-1069_3-5193525.html (Apr. 16, 2004).

[189] *Id*.

[190] *Id*.

[191] EPCGLOBAL, GUIDELINES ON EPC FOR CONSUMER PRODUCTS, *at* http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html (last visited July 11, 2004).

[192] *Id*.

[193] PROCTER & GAMBLE, *P&G Position on Electronic Product Coding (EPC)*, *at* http://www.pg.com/company/our_commitment/privacy_epc/epc_position.jhtml (last visited July 25, 2004).

Furthermore, existing laws already protect consumer privacy regardless of the technology employed to invade it. For example, California, like most jurisdictions, recognizes the privacy torts first proposed by Warren and Brandeis and later articulated by Prosser.[194] These four privacy torts are recognized in the Second Restatement of Torts.[195]

The type of surreptitious tracking RFID might facilitate would be covered by the tort for unreasonable intrusion upon the seclusion of another. For liability to exist under this tort, there must be an "intentional intru[sion] . . . upon the solitude or seclusion of another," and the intrusion must be of a kind that is "highly offensive to a reasonable person."[196] This tort generally does not apply when the individual is in the public eye.[197] Yet, this is not a hard and fast rule. Solitude does not depend on the victim's location, but rather on the victim's expectation of privacy and the kind of invasion that took place.[198]

[194] *See* Shulman v. Group W Productions, Inc., 955 P.2d 469 (Cal. 1998); Alim v. Superior Court, 229 Cal. Rptr. 599 (Cal. App. 3d Dist. 1986).

[195] The Second Restatement of Torts states:

(1) One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other.
(2) The right of privacy is invaded by
(a) unreasonable intrusion upon the seclusion of another ... or
(b) appropriation of the other's name or likeness ... or
(c) unreasonable publicity given to the other's private life ... or
(d) publicity that unreasonably places the other in a false light before the public....

RESTATEMENT (SECOND) OF TORTS § 652A (1977).

[196] *Id*. § 652B. Whether the information is publicized is irrelevant for this tort. Liability depends solely upon whether the individual's solitude was intruded upon. Id. § 652B cmt. a.

[197] *Id*. § 652B cmt. c.

[198] *Id*.; *See also* Med. Lab. Mgmt. Consultants v. Am. Broad. Cos., 306 F.3d 806, 812-13 (9th Cir. 2002).

California's constitution also recognizes a right to privacy.[199] The provision is self-executing and confers an individual right of action.[200] In *White v. Davis*, the California Supreme Court found that the main purpose of the constitutional grant of privacy is to tackle "the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society."[201] Specifically, the Court cited legislative history explaining that the constitutional amendment was meant to address concerns such as the "[c]omputerization of records [that] makes it possible to create 'cradle-to-grave' profiles of every American," as well as the race to compile ever more "extensive sets of dossiers of American citizens."[202] Not only does the constitutional right protect against government intrusion, but it extends to business misuse of information as well.[203]

Among the Joint Statement's list of RFID practices that should be "flatly prohibited" is, "merchants must be prohibited from forcing or coercing customers into accepting. . . RFID tags in the products they buy."[204] But forcing or coercing persons into doing anything against their will is already tortious conduct. However, a series of proposed RFID guidelines recently issued by EPIC sheds more light on how many privacy advocates define "force." That document states

[199] CAL. CONST. art. I, § 1. Many other states also protect privacy in their state constitutions. ALASKA CONST. art. I, § 22 ("The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section."); ARIZ. CONST. art. II, § 8 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law."); MONT. CONST. art. II, § 10 ("The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest."); WASH. CONST. art. I, § 7 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law."); FLA. CONST. art. I. § 12; HAW. CONST. art. I, §§ 6-7; ILL. CONST. art. I, §§ 6, 12; LA. CONST. art. I, § 5; S.C. CONST. art. I, § 10.

[200] White v. Davis, 533 P.2d 222, 234 (Cal. 1975).

[201] *Id*. at 233.

[202] *Id*.

[203] *Id*. *See also* Porten v. University of San Francisco, 64 134 Cal. Rptr. 839 (Cal. Ct. App. 1976) (student stated constitutional cause of action for invasion of privacy by private university).

[204] Joint Statement, *supra* note 88.

that merchants shall not "[c]oerce individuals to keep tags turned on after purchase for such benefits as warrantee tracking, loss recovery, or compliance with smart appliances."[205]

The law usually recognizes the requirement of action X in exchange for service Y not as coercion, but as a trade. What regulations such as the proposed EPIC guidelines seek is not privacy protection, but an entitlement or a wealth transfer. They want privacy-sensitive consumers to receive the good (loss recovery, smart appliance compatibility) without having to pay the attendant cost in privacy.[206] The effect of such a rule is to negate the lower prices made possible by technology such as RFID.[207]

RFID-specific laws to protect consumer privacy from businesses are unnecessary because existing contract, tort, and statutory privacy laws work. To single out RFID for special treatment might well be to kill it. Given the technology's precarious position today, removing any incentive for its adoption might spell its doom.

C. Checking Government RFID Snooping

As we have seen, the main RFID threat from government is the imposition of a mandatory national identifier. Such a mandate, while potentially unwise, is likely not unconstitutional.[208] Any check against such a system will have to be political. In the meantime, existing legal checks will restrain government surveillance using RFID where there is an expectation of privacy. Existing statutory privacy provisions, like the California Constitution,

[205] EPIC, *supra* note 185, at 3.

[206] Kent Walker, *The Costs of Privacy*, 25 HARV. J.L. & PUB. POL'Y 87, 114-117 (2001) (describing the free-rider problem that privacy legislation creates).

[207] *See id*. at 117.

[208] *See generally* A. Michael Froomkin, *The Uneasy Case for National ID Cards* (Mar. 2004), *available at* http://www.law.miami.edu/~froomkin/articles/ID1.pdf.

include protection from government snooping.[209] More importantly, Fourth Amendment law also curbs government high-tech surveillance powers.

In *Kyllo v. United States*,[210] the Supreme Court held that the use without a warrant of a thermal imaging device to scan the level of heat emanating from within a home constituted an unreasonable search under the Fourth Amendment.[211] The Court held that a search occurs when sense-enhancing technology obtains information "that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,'" and the technology used "is not in general public use."[212] In contrast, the Court in *United States v. Knotts*,[213] found radio frequency tracking not to be a violation of the Fourth Amendment. In that case, police placed a "beeper"—effectively a radio transmitter—on a container of chemicals that the defendant purchased.[214] The police used the beeper's signal to track the defendant to his cabin, where police found a drug lab.[215] The Eight Circuit Court of Appeals found use of the beeper to be an unreasonable search under the Fourth Amendment, and reversed the defendant's conviction.[216] But relying on *Katz v. United States*,[217] the Supreme Court reversed the appeals court, holding

[209] *See supra* note 199.

[210] 533 U.S. 27 (2001).

[211] *Id*. at 40-41.

[212] *Id*. at 34 (internal citation omitted). It should be noted that the dissenting opinion took issue with the holding's requirement that a technology must be "not in general public use" before its use can be considered a search. This is "somewhat perverse," the dissent said, because "the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available." *Id*. at 47 (Stevens, J., dissenting).

[213] 460 U.S. 276 (1983).

[214] *Id*. at 278.

[215] *Id*. at 278-79.

[216] *Id*. at 279.

[217] 389 U.S. 347 (1967).

that there is no reasonable expectation of privacy when traveling in an automobile on public roads.[218]

The rule therefore seems to be that radio frequency tracking is allowed without a warrant, unless it impinges on a constitutionally protected space—chief among them the home.[219] Reinforcing this analysis is *United States v. Karo*,[220] which also involved police placing a beeper on a container of chemicals to track a defendant's movements.[221] While again holding that the police's covert placement of a beeper on a container was not a search, the Court recognized Fourth Amendment protection when the beeper moved out of a public place and into a private space.[222]

CONCLUSION

RFID holds great potential to revolutionize not just the logistics business, but many other industries as well. Successful implementation would mean increased convenience and lower prices for consumers. But this will only happen if technological hurdles can be overcome, and if a business case can in fact be made for widespread use of RFID.

Although new technologies commonly elicit exaggerated privacy concerns, informed concerns should be taken seriously. However, until those fears are proven sound, legislators and regulators should resist constraining the use of RFID technology. Otherwise, they risk distorting or aborting what could be a very beneficial development. Existing law and, more importantly, consumer attitudes and the market forces they spawn will restrain undesirable use of RFID.

[218] *Knotts*, 460 U.S. at 281-82.

[219] Kyllo v. United States, 533 U.S. 27, 34 (2001) (noting that the home is an especially protected place under the Fourth Amendment).

[220] 468 U.S. 705 (1984).

[221] *Id*. at 708-710.

[222] *Id*. at 714.