WHERE WILL CONSUMERS FIND PRIVACY PROTECTION FROM RFIDS?: A CASE FOR FEDERAL LEGISLATION

SERENA G. STEIN[1]

ABSTRACT

With the birth of RFID technology, businesses gained the ability to tag products with practically invisible computer chips that relay information about consumer behavior to remote databases. Such tagging permits retailers and manufacturers to track the purchases, identities, and movements of their customers. In the absence of enforceable regulations, society risks being subjected to an unprecedented level of Orwellian surveillance. This iBrief addresses consumer privacy concerns stemming from the proliferation of RFID technology. It discusses why tort law, state legislation, FTC guidelines, and proposed regulations are insufficient methods to alleviate consumer privacy concerns and suggests amending various federal privacy laws, thereby prohibiting the underlying RFID tracking behavior.

INTRODUCTION

¶1 A problem has arisen at the intersection of privacy and technology. There is "an amazingly ambitious scheme to infest the entire physical infrastructure of the planet with a spray-on global blanket of Internet interactivity."[2] This "global blanket" is comprised of small data chips placed in moveable objects across the world that wirelessly communicate information about objects and their purchasers to anyone who has the technology to track it. The idea for the product-tracking technology was developed in 1997 as a result of the popularity of Oil of Olay's ColorMoist Hazelnut No. 650.[3] The inventor was neither a government agency nor an engineer. Rather, it was Kevin Ashton, a brand manager for Proctor &

---

[1] J.D. candidate at Duke University School of Law, 2008; B.S., Cornell University, 2004. I am grateful to Professor Sarah Ludington for her guidance and to the *Duke Law and Technology Review* staff members for their assistance.

[2] Bruce Sterling, *Preface* to KATHERINE ALBRECHT & LIZ MCINTYRE, SPYCHIPS: HOW MAJOR CORPORATIONS AND GOVERNMENT PLAN TO TRACK YOUR EVERY MOVE WITH RFID, at xi (2005).

[3] Cathy Booth-Thomas, *The See-It-All Chip*, TIME.COM, Sept. 22, 2003, http://www.time.com/time/magazine/article/0,9171,1005756-1,00.html.

Gamble.[4] Ashton, attempting to resolve a supply-chain quandary over the overwhelming popularity of lipstick, determined that placing a small chip, known as a Radio Frequency Information Device (RFID), on all lipstick packages would solve his stocking dilemma. He tested his idea in Broken Arrow, Oklahoma. When a customer removed the lipstick from the shelf, the RFID on the product's packaging sent information to databases in Cincinnati, informing Wal-Mart of reordering needs.[5] While RFID technology helped solve Wal-Mart's and other retailers' stocking problems, it also opened a Pandora's Box of privacy issues. Currently, there are no enforceable laws to control the spying and tracking actions of businesses and private individuals. Without regulations, the use of RFID chips in consumer products raises fears that "consumer behaviors" will be monitored, "third-party surveillance" will occur, "customer relationship[s]" will be managed, and individuals' identities and locations will be susceptible to constant monitoring.[6]

¶2 This iBrief will address the issues surrounding consumer privacy and RFIDs. Specifically, Part I will discuss the basic principles of RFID technology, detailing the various components of RFIDs and discussing how the technology functions as a communication device. Part II will address the scope of RFID use in the commercial environment, including its efficiencies and inefficiencies. Part III will evaluate the intrusion upon

---

[4] Ashton then left Proctor & Gamble to run the Auto-ID Center at MIT, where RFID standards are set. Kevin Maney, *RFID: Robot for Infinite Decluttering?*, USATODAY.COM, Oct. 6, 2004, http://www.usatoday.com/money/industries/technology/maney/2004-10-05-maney_x.htm. Ashton is now working at ThingMagic, an RFID start-up. *Id.* It should also be noted that RFID technology was initially used in World War II by the British army as radar-like devices to identify friendly aircrafts. Laura Hildner, *Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level*, 41 HARV. C.R.-C.L. L. REV. 133, 133 (2006) (citing *Radio Frequency (RFID) Technology: What the Future Holds for Commerce, Security and the Consumer: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 108th Cong. 10 (2004) (statement of Sanjay Sarma, Associate Professor of Mechanical Engineering, Massachusetts Institute of Technology)), *available at* http://www.law.harvard.edu/students/orgs/crcl/vol41_1/hildner.pdf.

[5] Cédric Laurant**,** Policy Counsel of the Elec. Privacy Info. Ctr.**,** Testimony on Radio Frequency Identification (RFID) Technology: What the Future Holds for Commerce, Security, and the Consumer (July 14, 2004), *available at* http://www.epic.org/privacy/rfid/rfidtestimony0704.html (citing *Chipping Away at Your Privacy,* Chi. Sun-Times, Nov. 9, 2003, at 36).

[6] STAFF OF THE FED. TRADE COMM'N, RADIO FREQUENCY IDENTIFICATION: APPLICATIONS AND IMPLICATIONS FOR CONSUMERS 1–2, 14 (2005), http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf.

seclusion tort as a theory of privacy protection and criticize the inability of this tort to keep pace with technological developments. Part IV will detail the challenges of using tort law to redress RFID offenses. Part V will analyze the various approaches of protecting consumers' privacy from RFID tracking, including legislation at the state level and regulation proposals from privacy advocates. Lastly, Part VI will provide suggestions for the most effective RFID legislation and the steps necessary for implementation of that legislation.

ANALYSIS

I. WHAT ARE RFIDS? HOW DO RFIDS WORK?

¶3 RFID technology is an automatic identification system that identifies objects, collects data, and transmits information about the object through a "tag." A device called a reader extracts and processes the information on the tag. Experts characterize RFIDs as devices "that can be sensed at a distance by radio frequencies with few problems of obstruction or misorientation."[7] In essence, RFIDs are wireless barcodes.[8] However, unlike typical barcodes, which are identical for all common products, each RFID has a unique identification. Therefore, every individually tagged item has a different barcode sequence. Typical barcodes also require unobstructed paths for scanning, whereas RFIDs can be scanned through solid objects.[9] RFIDs have communication signals that facilitate data storage on RFID tags and enable the stored information to be gathered electronically—hypothetically permitting, for example, Coca-Cola to have a database storing information about the life cycle of a Coke can. The database would contain tracking details from the moment the can is manufactured through its processing at a garbage dump—since RFID readers can be attached to garbage trucks. Between the birth and death of a customer's Coke can, the RFID tags would tell the Cola-Cola Company where and when the Coke was purchased, what credit card the Coke was purchased with, and, in turn, the identity of the purchaser. Even if the customer did not purchase the Coke with a credit card, state issued ID cards equipped with RFID technology could relay the customer's identity to RFID readers as he or she leaves the store.[10] Coca-Cola's final product of

---

[7] KATHERINE ALBRECHT & LIZ MCINTYRE, SPYCHIPS 13 (Nelson Current 2005) (quoting Raghu Das, *RFID Explained: An Introduction to RFID and Tagging Technologies*, ID TECHEX (2003). http://idii.com/wp/IDTechExRFID.pdf.

[8] RFID chips can be contrasted with barcodes, which use "optical line of sight." *Id*.

[9] *Id.*

[10] *See* Real ID Act of 2005, Pub. L. No. 109-13, 231 Stat. 119 (2005), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_public_laws&docid=f:publ013.109

the RFIDs' communications is a database of the life cycles of individual cans of Coke and personal information about their purchasers.[11] With this myriad of information, Coca-Cola has the ability to individually market to each of the 1.3 billion daily Coca-Cola consumers.[12]

¶4 There are three components of an RFID that permit the life cycle of a Coke can to be tracked: a chip, an antenna, and a reader. Together, the chip and the antenna are called a tag. A unique identification number, called an Electronics Product Code, is encoded in a small silicon chip that is typically smaller than three square inches.[13] The antenna, which can take the form of many shapes, radiates from the chip.[14] The antenna sends out radio signals that trigger the tag and permit information to be written onto and read from it.[15] The third component of an RFID is the reader. Also called the scanning device, the reader communicates with the tag through its own antenna.[16] Once an RFID tag comes within a few feet of the reader, the tag's antenna finds the reader's signal and directs the energy to the chip.[17] The chip then beams its unique identification number and other information stored on the chip to the reader. The reader then processes the information and typically relays the data to a database where it can be tracked and stored. Readers range in price from $20 to $1000. One variety, costing $150, is even adaptable to PDAs.[18] The low cost and ability to store a reader in the PCMCIA slot of a PDA permits businesses and individuals to own and use readers at their leisure.

¶5 There are passive and active tags. Passive tags are dormant until a reader beams the tag. Scanning by the reader activates communication between the devices. Active tags, on the other hand, are simply passive tags with an energy source, permitting them to continually transmit information,

---

(authorizing Department of Homeland Security to require state ID cards and drivers licenses to be equipped with RFID technology).

[11] While database storage poses an entire privacy issue on its own, exploration of database privacy is beyond the scope of this iBrief.

[12] The Coca-Cola Company, http://www.thecoca-colacompany.com/citizenship/our_business.html (last visited Feb. 15, 2007).

[13] The smallest chip, produced by Hitachi, is 0.3 square millimeters. *Hitachi Unveils Smallest RFID Chip*, RFID J., Mar. 14, 2003, http://www.rfidjournal.com/article/articleview/337/1/1/.

[14] ALBRECHT & MCINTYRE, *supra* note 7, at 14.

[15] David Flint, *Everything With Chips!*, BUS. L. REV., Mar. 2006, 73, 73.

[16] STAFF OF THE FED, *supra* note 6, at 4 (citing RSA Laboratories, http://www.rsasecurity.com/rsalabs/ (last visited Feb. 15, 2007)).

[17] ALBRECHT & MCINTYRE, *supra* note 7, at 16.

[18] *Get RFID Readers in a Flash*, RFID J., Apr. 22, 2003, http://www.rfidjournal.com/article/articleview/393/1/1/; *Toppan to produce $20 RFID Reader*, RFID J., Jan. 23, 2003, http://www.rfidjournal.com/article/articleview/279/1/1/.

without the activation of a reader. The cost for a passive tag can be as low as a few cents, and passive tags are typically priced between $0.20 and $0.40.[19] From a cost standpoint, the tags' low cost permits essentially all merchandise to be tagged with RFIDs. Although passive tags appear *passive*, by installing readers at various entrance points, including store entrances and freeway exits, the tags are essentially functionally *active*.[20] Locating the whereabouts of persons and objects simply requires scanning passive tags at these points of entrance. Because readers can scan multiple tags simultaneously, one reader can capture a great deal of location and information data in a short span of time.

II. HOW ARE RFIDS USED?

¶6 RFIDs are currently used in many ways, including, "livestock management[,] 24 hour patient monitoring[,] authentication of pharmaceuticals[,] tracking consignments in a supply chain[,] remote monitoring of critical components in aircraft[, and] monitoring the safety of perishable food."[21] Advocates of RFID technology, including retailers and manufacturers, praise the increased functionality and efficiency that will likely ensue from using RFIDs. Once all products are individually tagged, shoppers are expected to be able to purchase items without checking-out. This should be possible since RFID readers will be able to scan every item as the customer exits the store and charge an RFID credit card, thereby simultaneously increasing efficiency and possibly reducing shoplifting. Other RFID uses include easy monitoring of product recalls, tracking lobsters for conservation purposes, and purchasing products with transaction-free payment systems.[22] Additionally, in October 2003, the Department of Defense set standards mandating suppliers to place RFID

---

[19] *RFID System Components and Costs*, RFID J., http://www.rfidjournal.com/article/articleprint/1336/-1/129/ (last visited Feb. 15, 2007).

[20] ALBRECHT & MCINTYRE, *supra* note 7, at 5.

[21] Viviane Reding, Member of the European Commission responsible for Information Society and Media, Address at EU RFID 2006 Conference: Heading for the Future, RFID: WHY WE NEED A EUROPEAN POLICY, 1, 3 (Oct. 16, 2006), *available at* http://europa.eu.int/rapid/pressReleasesAction.do?reference=SPEECH/06/597&format=PDF&aged=0&language=EN&guiLanguage=en; *see also* MICHAEL J. TAVILLA, *RFID*, NAT'L ELEC. COMMERCE COORDINATING COUNCIL 5-7 (2005), http://rfidprivacy.mit.edu/access/pdfs/report-ec3.pdf.

[22] Flint, *supra* note 15, at 1.

tags on all packaging for the Department of Defense.[23] Thus, RFIDs can be used to increase efficiency and safety.

¶7 The RFID uses enumerated above, however, are not the uses that drive privacy concerns. Rather, it is the spying on individuals and the profiling of their identities that are at issue. According to a study provided by Auto-ID Center, seventy-eight percent of consumers are "extremely or very concerned" about the uses of RFID technology[24]—likely because they fear customer profiling and care about keeping their identities private from businesses. These concerns stem from the lack of current laws protecting consumers from data collection and sharing. Some companies cannot be trusted with the data that they collect, and existing privacy laws do not help individuals hide the information they expect to be concealed from the public.[25] A consumer who purchases RFID tagged items is vulnerable to various types of surveillance. For example, consider customers carrying RFID-enabled health-insurance cards in their wallets purchasing shopping carts full of junk food at the grocery store. If the health insurance company placed RFID readers at grocery store entrances, the reader would activate the RFID tag in the consumers' wallets and collect information about their recent grocery purchases. From the health-insurance card the insurance carrier could determine the customers' identities and learn that they are prone to diabetes. When the junk food purchases are aggregated into their policy files, the purchases could trigger increases in the consumers' health insurance.

¶8 The capabilities of RFID technology now permit businesses to snoop into the lives of customers in ways that were never before possible.[26]

---

[23] PRESS RELEASE, US DEP. OF DEFENSE, DOD ANNOUNCES RADIO FREQUENCY IDENTIFICATION POLICY, UNITED STATES DEPARTMENT OF DEFENSE NEWS RELEASE, (OCT. 23, 2003), http://www.defenselink.mil/releases/2003/nr20031023-0568.html.

[24] ALBRECHT & MCINTYRE, *supra* note 7, at 154 (quoting PHYLLIS L. KIM, FLEISHMAN-HILLARD, AUTO ID CENTER COMMUNICATIONS (2001), http://cryptome.org/rfid/pk-fh.pdf); *see* Beth Bacheldor, *Study: RFID Not Well-Known by Consumers*, INFO.WK., June 24, 2004, http://www.informationweek.com/story/showArticle.jhtml?articleID=22101950.

[25] *See* Anick Jesdanun, *3 AOL Subscribers Sue Over Data Release*, ABC NEWS, Sept. 25, 2006, http://abcnews.go.com/Technology/wireStory?id=2489737; Complaint, Kasadore Ramkisson v. AOL, No. 06-5866 (N.D.Cal. Sept. 22, 2006) (bringing suit under the Electronic Communication Privacy Act, 18 U.S.C. § 2702, for posting AOL users search queries).

[26] EPIC RFID Privacy Page, http://www.epic.org/privacy/rfid/ (last visited Feb. 15, 2007); *see* U.S. Patent App. 20020165758 (filed May 3, 2001), *available at* http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220020165758%22.PGNR.&OS

The NCR Corporation[27] stated that RFID-enabled loyalty cards permit businesses to identify customers and change the prices of items based on the purchasing profile of the customer.[28] A clothing retailer could tag purchased garments with customers' credit card information and determine how much money they are likely to spend as they enter the store.[29] Sales representatives could quickly target or avoid customers depending on their historical purchasing habits.[30] RFID data collection could be used as evidence in divorce trials, helping prove where and when a spouse was being unfaithful.[31] Thieves could use RFID devices to determine if their culprits are carrying expensive items in their purses.[32] As these examples show, "the ability to remain anonymous is eroded."[33] With personal information available to anyone who has a reader, privacy will soon become obsolete unless there are laws regulating the potential for Orwellian surveillance.

III. DO CONSUMERS HAVE A RIGHT TO PRIVACY FROM RFIDS UNDER TORT LAW?

¶9 Consumers have a right to privacy under the common law tort of intrusion upon seclusion only when two elements are satisfied. First, the information must be pulled in places that are highly "offensive or objectionable to a reasonable man," and second, "the thing into which there is prying or intrusion [is] entitled to be, private."[34] Intrusion upon seclusion is a tort protecting individuals against "intentional[] intru[sion], physically or otherwise, upon the solitude or seclusion of another or his private affairs

---

=DN/20020165758&RS=DN/20020165758 (describing a method for tracking identities and characteristics of individuals to "monitor movement throughout the store."); U.S. Patent No. 6,659,344 (filed Dec. 6, 2000), *available at* http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=6659344.PN.&OS=PN/6659344&RS=PN/6659344 (describing a method of gathering data of supermarket shoppers behaviors by placing readers on shopping carts in order to "take specific responses to the actions of the shoppers").

[27] "NCR Corporation . . . along with its subsidiaries provides technology and services that help businesses interact, connect and relate with their customers." Google Finance, http://finance.google.com/finance?q=NCR (last visited Feb. 15, 2007).

[28] ALBRECHT & MCINTYRE, *supra* note 7, at 74.

[29] *See id.* at 74–75.

[30] *See id*.

[31] Declan McCullagh, *RFID Tags: Big Brother in Small Packages*, CNET NEWS.COM, Jan. 13, 2003, http://news.com.com/2010-1069-980325.html.

[32] *Id.*

[33] *Id.*

[34] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 390–91 (1960).

or concerns . . . if the intrusion would be highly offensive to a reasonable person."[35] Samuel Warren and Louis Brandeis introduced the theory of the right to privacy in 1890, proclaiming that "[t]he right to life has come to mean the right to enjoy life,—the right to be let alone."[36] When people are in the seclusion of their home, they are undoubtedly entitled to privacy.[37] However, an individual's expectation of privacy is not limited to inside the home.[38] A reasonable expectation of privacy can exist in one's shopping bag in a store,[39] when one withdraws money from a bank account,[40] and in a phone booth.[41] In order for the plaintiff to have a claim, the defendant must have "penetrated some zone of physical or sensory privacy surrounding, or obtained unwanted access to data about, the plaintiff."[42]

¶10 In the context of RFIDs, there are some situations where gathering information from RFID tags violates consumers' privacy expectations. For example, a consumer does not have a reasonable expectation of privacy when carrying RFID equipped items in a transparent shopping cart. However, once the items are placed in an opaque bag, a right to privacy immediately arises.[43] If a business or third-party gathers data about the items once the items are no longer visible to the naked eye, there is an objective invasion of privacy.[44] Gathering information stored in the RFID tag in a winter jacket worn in public is also not an invasion of privacy, yet pulling data off undergarments is intrusive.[45] However, since the home is always considered a private place, once an active RFID tag enters the home, any information gathered, including information from the winter jacket, immediately offends the principles of privacy. Protecting consumers from unreasonably intrusive actions of businesses requires that RFID tags become unreadable once they enter private places. However, the fundamental nature of the technology does not harmonize with this privacy

---

[35] RESTATEMENT (SECOND) OF TORTS § 652B (1977).
[36] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4. HARV. L. REV. 193, 193 (1890).
[37] *See* Prosser, *supra* note 34, at 392; *see also* DeMay v. Roberts, 9 N.W. 146, 149 (Mich. 1881) (finding a right to privacy in one's apartment).
[38] Katz v. United States, 389 U.S. 347, 359 (1967).
[39] Prosser, *supra* note 34, at 389 (citing Sutherland v. Kroger Co., 110 S.E.2d 716 (W. Va. 1959)).
[40] Nader v. General Motors, 255 N.E.2d 765 (N.Y. 1970).
[41] *Katz*, 389 U.S. at 359.
[42] Shulman v. Group W Prods., Inc., 955 P.2d. 469, 490 (Cal. 1998).
[43] *See* Prosser, *supra* note 34 at 390-91.
[44] *Id*.
[45] *See* Restatement (Second) of Torts § 652B cmt. c (1977) ("Even in a public place . . . there may be some matters about the plaintiff, such as his underwear or lack of it, that are not exhibited to the public gaze; and there may still be an invasion of privacy when there is intrusion upon these matters.").

goal because RFID readers do not scrutinize whether the information is considered private before it gathers data from the tag.

¶11 For the tort of intrusion upon seclusion, the "highly offensive" element normally requires more than simple visual surveillance or photography in a public place unless the individual is attempting to keep his actions private.[46] Thus, the moment an individual enters a private place, actions that were not considered highly offensive because they occurred in public should be immediately deemed highly offensive. It follows that any item entering the home with a readable RFID tag should be highly offensive to the reasonable person. However, with new and continuously evolving technologies, what individuals consider offensive and private is continually changing. For example, in *Dwyer v. American Express Co.*,[47] the court rejected an American Express cardholder's claim of intrusion upon seclusion when American Express data-mined the plaintiff's spending patterns and sold the collected information to merchants.[48] The court stated:

> By using the American Express card, a cardholder is voluntarily, and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder's spending habits and shopping preferences. We cannot hold that a defendant has committed an unauthorized intrusion by compiling the information voluntarily given to it and then renting its compilation.[49]

¶12 With new technologies come new methods of consumer tracking and changing parameters for what may be considered highly offensive. These new methods of tracking are not considered intrusive simply because the nature of the technology requires consumer purchases to be recorded. If individuals make active decisions to use a credit card instead of cash—a voluntary act—their purchases can be tracked. Similarly, the gathering of information stored on RFID technology in consumer goods may not be deemed highly offensive depending on changing consumer expectations.

¶13 The ability to track an item and an individual at any time does not alone make the technology highly offensive. Rather, the ability of RFID technology to track an item becomes highly offensive where there is a reasonable expectation of privacy. With RFID technology third parties are able to secretly track individuals by "skimming" and "eavesdropping."[50]

---

[46] Sanders v. Am. Broad. Cos., 85 Cal. Rptr. 2d 909, 914–15 (1999) (citing *Shulman*, 955 P.2d. at 490).
[47] 652 N.E.2d 1351 (Ill. App. Ct. 1995).
[48] *Id.* at 1353.
[49] *Id.* at 1354 (emphasis added).
[50] Another major privacy issue with RFID tags, both in identification cards and consumer products, relates to private third parties skimming or eavesdropping.

Data that may otherwise not be available to third parties becomes readily obtainable at any place where there is an active RFID reader. Thus, the placement and presence of RFID tags in consumer goods permits the highly intrusive gathering of information when the items are in private places. Despite this issue, individuals will have a difficult time bringing a valid cause of action since they will not know when items they carry are equipped with RFID tags and whether the information is being procured when they have a reasonable expectation of privacy.

IV. WHAT CHALLENGES ARISE WHEN USING TORT LAW TO REDRESS RFID OFFENSES?

¶14 It is often difficult to meet the burden of proof required for intrusion upon seclusion.[51] There are some circumstances, including when the item is in public view, where gathering information from RFIDs is almost never tortious. There are other circumstances when the same act of information gathering is tortious. For example, in *Nader v. General Motors*, the court stated that "only 'overzealous' public surveillance is actionable."[52] It is difficult to argue that a small RFID chip, sewn into clothing seams, is "overzealous" public surveillance. Therefore, it is inaccurate to conclude that using RFID technology to collect data is highly offensive when the information can be gathered by means that are not "overzealous."[53]

¶15 Additionally, under the theory of intrusion upon seclusion, plaintiffs must prove damages, which could be difficult for this technology.[54] For a successful intrusion upon seclusion action against a business or individual that uses RFID technology, a plaintiff can "recover damages for (a) the harm to his interest in privacy resulting from the invasion; (b) his mental

---

Two Reports Criticize Security, Privacy Holes in RFID Technology, EPIC ALERT 13.22 (Electronic Privacy Information Center, Washington, D.C.), Nov. 1, 2006, http://www.epic.org/alert/EPIC_Alert_13.22.html ("Skimming occurs when information from an RFID chip is surreptitiously gathered by an unauthorized individual. Eavesdropping occurs when an individual intercepts data as it is read by an authorized RFID reader."). While third party interferences are mentioned, a detailed analysis of the issues of skimming and eavesdropping is beyond the scope of this iBrief.

[51] Adam J. Tutaj, *Intrusion Upon Seclusion: Bringing an Otherwise Valid Cause of Action into the 21st Century*, 82 MARQ. L. REV. 665, 666 (1998).

[52] *Id.* at 683 (quoting 255 N.E.2d 765,771 (N.Y. 1970)). In *Nader*, the defendants engaged in unauthorized surveillance of bank records. *Nader*, 255 N.E.2d at 765.

[53] Tutaj, *supra* note 51 at 666.

[54] Alan F. Blakley, Daniel P. Garrie, & Matthew J. Armstrong, *Coddling Spies: Why the Law Doesn't Adequately Address Computer Spyware*, 2005 DUKE L. & TECH. REV. 0025 (2005), http://www.law.duke.edu/journals/dltr/articles/2005dltr0025.html.

distress proved to have been suffered if it is of a kind that normally results from such an invasion; and (c) special damage of which the invasion is a legal cause."[55] The Restatement (Second) of Torts is silent on whether a plaintiff could receive restitution damages for the value that the defendant gained by intruding upon the seclusion of the plaintiff.[56] A separate cause of action may need to be brought for a plaintiff to receive restitution.

¶16 With respect to the amount of damages that make a cause of action feasible, a single plaintiff's legal claim against a retailer for scanning will probably not amount to enough relief for the claim to be justified, especially since punitive damages are not guaranteed. Further, since most individuals are not aware of the existence of RFID tags in their purchases,[57] and because the technology does not require any true physical imposition on the individual, retailers and manufacturers will not be pressured to cease their intrusive actions on scattered tort claims. In addition, from a plaintiff's or mass-tort perspective, it is not feasible to bring a suit against all manufacturers and retailers that use RFID technology. And, it is not effective for a plaintiff to bring suit against only one company because a cause of action against one business would not impinge on the actions of other businesses. To prohibit all retailers from using RFIDs in intrusive manners, the plaintiff would have to sue every retailer and plead for injunctive relief. While one win for the plaintiff may deter other possible defendants, a cost-benefit analysis by large companies using RFID technology would likely justify continued use.

¶17 RFID tracking is tortious under a theory of intrusion upon seclusion only when a reader pulls information from RFID tags when the item is located in a place where its owner has a reasonable expectation of privacy and when the action is highly offensive. While there are some situations where both elements of the tort of intrusion upon seclusion are satisfied, such as when the RFID is located in the privacy of one's home, there are many potentially intrusive uses of RFID for which it will be difficult for a plaintiff to prove the tortious conduct and establish harm. Furthermore, even if RFID technology is "overzealous" and even if it is practical for a plaintiff to bring a claim, courts have been reluctant to permit plaintiffs to use intrusion upon seclusion for technology claims in the twenty-first

---

[55] RESTATEMENT (SECOND) OF TORTS § 652H (1977).

[56] "One whose name, likeness or identity is appropriated to the use of another, under [Restatement (Second) of Torts] § 652C, may recover for the loss of the exclusive use of the value so appropriated." *Id.* at cmt. a. When there has been appropriation, the plaintiff may recover a value equal to that of which the defendant was enriched by the fraud. *Id.*

[57] A survey "conducted by Capgemini and National Federation found that 77% of consumers were not familiar with RFID." Bacheldor, *supra* note 24.

century.[58] As new technologies continue to enter the market, an industry sector approach to regulation is becoming the legal trend: Congress passes statutes for industry-specific technology to protect consumer privacy.[59] However, almost a decade after the birth of RFIDs, the technology has yet to be regulated.

V. WITHOUT TORT LAW, WHAT PROTECTS CONSUMERS?

¶18 The Federal Trade Commission (FTC), which governs RFIDs, currently permits companies to craft their own guidelines concerning the use of customer data collected through RFID technology.[60] As part of self-regulation, the FTC encourages businesses to notify consumers of the existence of RFIDs in their products and to inform customers of the type of data that is being collected and the data's intended use.[61] However, the FTC "has not taken any enforcement actions against any companies and has not compiled any statistics as to who is using RFID technology . . . ."[62] Under the current self-regulatory scheme, it is unlikely that the FTC will ever take enforcement actions because it can only enforce regulations that a company sets for itself and subsequently violates.[63] Thus, if a company does not establish standards for self-enforcement, then failing to notify the user of the existence of RFIDs will not be a violation and the FTC cannot take action. As there are very limited situations in which the FTC would have the ability to take enforcement actions, self-regulation is not an effective means of regulation.

¶19 Without current laws actively monitoring and regulating the actions of businesses' RFID uses, the information gathering and aggregation occurring as a result of RFID technology may expose customers to harmful invasions of privacy. Although state legislatures have begun efforts to legislate RFID technology at the state level and privacy advocates have set forth numerous state legislative proposals, federal regulation is ultimately needed to effectively protect consumers. The efforts at the state level have

---

[58] *See* White v. White, 781 A.2d 85 (N.J. Super. Ct. Ch. Div. 2001) (finding no reasonable expectation to privacy in e-mail).
[59] Hildner, *supra* note 4, at n.144 (listing industry-specific technologies).
[60] Jonathan Collins, *FTC Asks RFID Users to Self-Regulate*, RFID J., Mar. 10, 2005, http://www.rfidjournal.com/article/view/1437/1/1/; *see,* 5 U.S.C. §§ 41–58 (2000) (Federal Trade Commission Act).
[61] Collins, *supra* note 60.
[62] Claire Swedberg, *FTC Readies an RFID Report*, RFID J., Oct. 5, 2004, http://www.rfidjournal.com/article/articleprint/1151/-1/1/.
[63] Hildner, *supra* note 4, at 145 (noting further, that if FTC chooses to institute its own regulatory guidelines the investigation and negotiation before judicial review bodies would be burdensome to the FTC and likely cause lengthy procedural delays).

not been very successful and the proposals from advocacy groups are limited in scope. International regulatory regimes, while not perfect, may provide some guidance as to how the United States should tackle the RFID issue.

A. RFID Regulation at the State Level

¶20 In 2006, at least seventeen states introduced RFID-related legislation.[64] Georgia, New Hampshire and Wisconsin adopted RFID-related legislation while California and Rhode Island each vetoed RFID-related bills.[65] In 2005, privacy bills regulating RFIDs were introduced in twelve state legislatures.[66] Likewise, in 2004, several state legislatures actively sought RFID legislation.[67]

¶21 RFID legislation at the state level typically targets five different issues:

1. "Requir[ing] disclosure";
2. "Requir[ing] removal or deactivation";
3. "Prohibit[ing] linking RFID data to personal information";
4. "Prohibit[ing] use" in general; and
5. Criminalization.[68]

¶22 These state legislative measures, however, have not adequately addressed the privacy concerns raised by RFID technology for several

---

[64] *2006 Privacy Legislation Related to Radio Frequency Identification*, NEWS FROM THE STATES (National Conference of State Legislatures), Oct. 2006, http://www.ncsl.org/programs/lis/privacy/rfid06.htm.
[65] *Id.*
[66] *2005 Privacy Legislation Related to Radio Frequency Identification*, NEWS FROM THE STATES (National Conference of State Legislatures), Jan. 30, 2006, http://www.ncsl.org/programs/lis/privacy/rfid05.htm.
[67] *See* H.B. 32, 418th Gen Assem., Reg Sess. (Md. 2004); S.J.R. 10, 56th Leg., Gen. Sess. (Utah 2004), H.B. 1304, 2004 Sess. (Va. 2004); H.B. 314, 56th Leg. Gen Sess. (Utah 2004); H.B. 251, 56th Leg. Gen Sess. (Utah 2004); S.B. 867, 92nd Gen. Assem., 2nd Reg. Sess. (Mo. 2004); S.B. 1834, 2004 Reg. Sess., (Cal. 2004); H.B. 151, 2004 Sess. (Va. 2004). Maryland, Utah and Virginia's bill suggest guidelines for future legislation; Missouri's bills require labeling; Utah's bills require labeling and address the requirement for disabling the device; and California's bill addresses the use of personal information. Joshua Nelson, *State Legislatures Address Use of RFID Technology*, NEWS FROM THE STATES (National Conference of State Legislatures), Summer 2004, http://www.ncsl.org/programs/lis/CIP/CIPCOMM/summer04.htm.
[68] *2006 Privacy Legislation*, *supra* note 64.

reasons. First, no proposed legislation in 2006 confronted all of the alleged privacy and security issues associated with RFIDs. Second, a majority of the legislation presented limited situations where prohibition of data linking is enforceable.[69] Third, regulating RFID technology at the state level is inherently inefficient because customers who purchase goods in states where there are no RFID regulations or enforcement are not protected from retailers located within their home state. For example, if a consumer purchases a shirt in a state that does not require disclosure of the presence of RFID technology to consumers, when the consumer returns to his own home state, information could be read from the RFID tag in his clothing of which he is not aware. The consumer does not have the ability to know that information is being pulled from him, nor the opportunity, as some statutes permit, to allow him to request a copy of the information gathered and its intended use. Since RFID technology is used to track inventory nationally and manufacturers supply products to various states, regulating at state levels interferes with efficient commerce. This is not an effective way to protect the privacy of our nation's citizens or promote economy.

¶23 Currently, there is no federal legislation relating to RFIDs. The only federal action is a proposal for an RFID Caucus.[70] With legislation occurring at state rather than federal levels, the necessary protections for consumers have not been established by, let alone introduced to, Congress.

B. Proposals from Privacy Advocates

¶24 Preserving basic liberty rights of a society with technological advances requires a sensitive balance between creating stringent legal standards that protect individuals and relaxed regulations that do not deter innovation and efficiency. As a technology, RFIDs have the capability to increase efficiency in multiple arenas, especially the retail sector. The resulting privacy issues, however, are of prime concern. Privacy advocates have tried to protect consumer fears by proposing multiple regulations and model codes that place duties on businesses when using RFID technology in

---

[69] *Id.* (explaining that most bills permit exceptions to the prohibition of data linking when discussing state or federally issued identification cards).

[70] Rfidblogger, *Senators Form RFID Caucus*, RFID LAW BLOG, June 26, 2006, http://rfidlawblog.mckennalong.com/archives/federal-legislation-senators-form-rfid-caucus.html (stating that the purpose of the caucus is to "[p]rotect exciting new technologies from premature regulation or legislation in search of a problem."). There is also "[f]ederal legislation that details security provisions that must be in place for Federal Employee ID cards using contact and contactless smart cards." *CA State Legislation Update*, (Association for Automatic Identification and Mobility), Aug. 29, 2005, http://www.aimglobal.org/members/news/templates/rfid.asp?articleid=434&zoneid=3. However, these standards do not protect consumers.

their products. Each proposal attempts to address the privacy concerns of consumers by placing restrictions on businesses. Among these proposals are the Fair Information Practices, The RFID Right to Know Act of 2003, Electronic Privacy Information Center's Guidelines on Commercial Use of RFID Technology, and regulations in the international arena, all of which detail various means to achieve the requisite balance between efficiency and personal privacy.

1. Fair Information Practices

¶25 Fair Information Practices refers to the "manner in which entities collect and use personal information."[71] The first comprehensive use of Fair Information Practices appeared in 1973 in the United States Department of Health, Education and Welfare's report, *Records, Computers and the Rights of Citizens*.[72] Since then, Fair Information Practices have been used as the foundation for American privacy laws. While some organizations have fashioned proposed regulations based on Fair Information Practices, for the purposes of RFID privacy, Fair Information Practices simply create the basis for a model code detailing principles to safeguard information privacy. Fair Information Practices are founded on "five core principles of privacy protection": notice, choice, access, security, and enforcement.[73]

¶26 If the notion of Fair Information Practices expressly regulated RFID privacy, a retailer or manufacturer would set privacy regulations for information gathering and storage. The notice principle would require consumers to receive "clear and conspicuous notice of an entity's information practices before any personal information is collected from them . . . ."[74] To comply with the notice requirement, retailers would have to label items with tags or stickers warning the purchaser that the item is equipped with RFID technology. Further, the label would be required to mention the purpose of the RFID tag in the specific product, the type of data the tag collects, how the collected data is used, and the means by which the information is kept confidential. The choice principle provides consumers the right to determine how the information gathered about them is used after a transaction is complete.[75] This principle permits consumers to consent to the actions taken by the retailer. For instance, the consumer has the right to

---

[71] FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS, June 1998, http://www.ftc.gov/reports/privacy3/fairinfo.htm.
[72] *Id.* at n.27.
[73] FEDERAL TRADE COMMISSION, *supra* note 71.
[74] FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 14 (May 2000), http://www.ftc.gov/reports/privacy2000/privacy2000text.pdf.
[75] *Id.* at 15.

decide if the retailer can use his personal collected data for "secondary uses," such as marketing lists for other companies.[76] The access principle permits an individual the right to view the gathered information and dispute its accuracy such that incorrect data does not adversely affect the consumer based on the retailers' intended uses.[77] The security principle requires retailers to protect the gathered information.[78] This may require RFID encryption, tag removal once an item is purchased, and installation of database protection technology. Enforcement of the aforementioned guidelines is essential for consumers to feel comfortable when businesses use RFID technology.

¶27 While Fair Information Practices are composed of crucial principles that protect consumers from RFID threats, the application of these five standards is not the end all to regulating RFIDs. Fair Information Practices do not guarantee absolute consumer protection because information can still be collected from unsuspecting customers. Specifically, with regards to RFIDs, the principles do not account for the type of customer profiling that RFID technology allows. Even if a consumer purchases a product with a secure RFID tag (security), knows that the purchasing information will be gathered from the tag (notice), understands that the information will not be sold to a third party (consent), but does not remove the tag after purchase, the regulations of RFIDs are not entirely effective. Any RFID tag that remains on a product after tender jeopardizes the integrity of Fair Information Practices because the tracking continues to take place. RFID regulations should permit retailers to use RFID technology to increase supply-chain efficiency but not at the expense of consumer privacy. There is a privacy failure if all five principles are satisfied, yet a third party inside or outside the walls of a store can gather information from the RFID tag as a result of the information gathering and storage. Thus, Fair Information Practices are not an adequate means of RFID privacy regulation.

2. RFID Right to Know Act

¶28 The RFID Right to Know Act, created by Consumers Against Supermarket Privacy Invasion and Numbering ("CASPIAN"), stipulates mandatory labeling requirements for products equipped with RFID technology.[79] The act suggests amendments to current statutes as a means

---

[76] *Id.*
[77] *Id.* at 16.
[78] *Id.* at 18.
[79] Consumers Against Supermarket Privacy Invasion and Numbering: RFID Right to Know Act of 2003, http://www.nocards.org/rfid/rfidbill.shtml (last visited Feb. 15, 2007) ("[C]ommodities containing radio frequency identification tags bear labels stating that fact, to protect consumer privacy, and for other purposes.").

of protecting consumer privacy. These amendments include changes to Fair Packaging and Labeling Program,[80] Federal Food, Drug, and Cosmetic Act,[81] Federal Alcohol Administration Act,[82] Federal Cigarette Labeling and Advertising Act,[83] and Chapter 94—Privacy of Title 15 of the U.S. Code.[84] The proposed legislation amends the language in the aforementioned statutes to mandate clear and conspicuous labeling on any "consumer commodity or package" that includes an RFID tag.[85] The suggested amendment to Title 15, Chapter 94—Privacy, creates an additional subchapter titled "AGGREGRATION OF NONPUBLIC PERSONAL INFORMATION AND RADIO FREQUENCY INDENTIFICATION INFORMATION."[86] The proposed subchapter details that businesses shall not:

- "combine or link an individual's nonpublic information with RFID tag identification information beyond what is required to manage inventory."[87]
- "disclose to a nonaffiliated third party an individual's nonpublic information in association with RFID tag identification information."[88]
- "use RFID tag identification information to identify an individual."[89]

In addition, the subchapter requires the FTC to create standards to insure the integrity of the information gathering, security, and general harm caused by RFIDs.[90] Under the proposed legislation the FTC must also disseminate general educational information regarding RFIDs to consumers and businesses as well as enforcement.

¶29 Amendments to current statutes are a more effective means of protecting consumer privacy than Fair Information Practices. On the positive side, the RFID Right to Know Act provides detailed musts and must-nots by requiring notice on labels and prohibiting certain uses of private information. However, the Act also has limitations. The Act does not consider regulations of consumer products that are not food, drug,

---

[80] 15 U.S.C. § 1453 (2000).
[81] 21 U.S.C. § 321 (2000).
[82] 27 U.S.C. § 215 (2000).
[83] 15 U.S.C. § 1333 (2000).
[84] 15 U.S.C. Ch. 94.
[85] RFID Right to Know Act, *supra* note 79.
[86] *Id.*
[87] *Id.*
[88] *Id.*
[89] *Id.*
[90] *Id.*

cosmetics, alcohol, and cigarettes. While these types of consumer goods, most of which are regulated by the FDA, are all commonly equipped with RFID technology, it is the items that consumers carry with them in public, specifically clothing and shoes, that require the most stringent regulations, and are not addressed by the Right to Know Act. Also, one is more likely to receive poor customer service based on purchasing habits in a retail store than in grocery stores. Amending legislation for specific consumer goods is not an efficient way to regulate consumer privacy. Although regulations at the federal level are crucial, regulating individual products one by one is not effective. The proposed amendment to Chapter 94-Privacy of Title 15 of the U.S. Code does not regulate specific products, yet amendments to this section alone are also insufficient. While it is important for information linked to individuals to be protected, it is just as crucial to address in detail the general issues proposed by Fair Information Practices.

3. Electronic Privacy Information Center (EPIC)

¶30 EPIC, a leading public interest research center on privacy issues has formed *Guidelines on Commercial Use of RFID Technology.*[91] The guidelines require businesses to notify potential RFID tag holders of the presence of tags and readers and signal the tag holder when the reader is pulling information from the tag.[92] The guidelines stipulate that the tags must be removable and require an analysis to ensure that there are no less intrusive means to achieve the same goal. If less intrusive means are not available, the user must obtain written consent after disclosing the purpose, extent and use of the data collection. According to EPIC's guidelines, under no circumstance may personal identification data be distributed to third parties.[93] Additionally, the collected data must be secure, information relating to data collecting policies must be available to tag holders, and an individual's personal data may be retrieved upon written notice to the business. [94]

¶31 These regulations provide a thorough application of privacy laws to potential RFID uses. However, the guidelines do not protect an individual's privacy outside the commercial arena and create high transaction costs for businesses, which would likely be transferred to the consumer. From the standpoint of data collection by corporations, the stringent limitation on use may be a disincentive to employ RFID technology at all. While the burden to protect privacy in the commercial environment is rightfully placed on the retailer and the manufacturer, the EPIC guidelines give consumers

[91] *See Guidelines on Commercial Use of RFID Technology*, EPIC.org, July 9, 2004, http://www.epic.org/privacy/rfid/rfid_gdlnes-070904.pdf.

[92] *Id.* at 2–3.
[93] *Id.* at 3.
[94] *Id.*

unlimited authority to request information regarding their collected personal data from the businesses using RFID technology. There are two issues with this provision of the proposed regulation that affect the business and the consumer. First, if consumers wish to continually view data collected by a business, they would have to write multiple letters to the business to keep track of the personal information the business has gathered. Second, the business would be forced to aggregate data in way that accommodates generating reports for every single consumer. This aggregation would require information to be stored in such a way that requires data to be attached to a consumer's identity—which is contrary to the goals of RFID regulation. In general, EPIC's proposal would increase costs to business without the balanced benefits to the consumer.

C. International Approaches

¶32 At the International Conference of Data Protection & Privacy Commissions a resolution of the required standards for RFID use was adopted. The standards require:

- an analysis to ensure that less intrusive means in achieving the same goal are not possible;
- that the gathered information is "open and transparent";
- that any collected data is stored only until the purpose of the information gathering is complete; and
- that the data on the tags are destroyable.[95]

¶33 The European Union also has its own regulations in place that protect privacy. In fact, there are "strong laws governing the use of data gathered on consumer[s]."[96] Although the regulations were not initially enacted for the specific uses of RFIDs, the preexisting laws protect personal data associated with RFIDs. In Europe, protections are in place because of the limited range of frequencies for RFID readers.[97] Additionally, the

---

[95] *Resolution of Radio Frequency Identification*, International Conference of Data Protection & Privacy Commissions, Nov. 20, 2003, http://www.privacyconference2003.org/resolutions/res5.DOC.

[96] Reuven R. Levary, David Thompson, Kristen Kot & Julie Brothers, *RFID, Electronic Eavesdropping and the Law*, RFID J., Feb. 14, 2005, http://www.rfidjournal.com/article/articleview/1401/1/128.

[97] "In the US, there are 60 channels that can be used for deploying RFID readers, however in Europe there are only 10 channels. This is because a 26 MHz spectrum is available in the US but only 2 MHz is available in Europe." *RFID in Europe*, RFID GAZETTE, Sept. 23, 2005, *available at* http://www.rfidgazette.org/2005/09/rfid_in_europe.html.

"personal data must be processed fairly and lawfully."98 In the United Kingdom, for example, fair and lawful processing of data requires notice to the consumer and either "consent, contractual necessity, [or] legitimate interest."[99] The "e-privacy directive" also requires there to be individual notice of the data uses, ability to withdraw consent, and capability to prevent temporary data processing to track consumers' locations.[100]

¶34 These standards are in line with those of the Fair Information Practices as a means to ensure uniformity within international borders. However, the international resolution is more restrictive on business than Fair Information Practices and provides greater protections to consumers. A balancing test should be the baseline for RFID regulation in the United States. A balancing test will restrict businesses' uses of RFID technology in unnecessary situations, while not inhibiting the needed increased efficiencies. A balancing test also requires businesses to contemplate their infringement on their customers' privacy before implementing unnecessary tracking standards. Additionally, the approach the European Union has taken to limit information gathering by restricting the frequencies available to RFID is an effective way to limit RFID tracking without banning all uses of the technology.

VI. A SOLUTION.

¶35 According to Kevin Ashton, "[i]t's game over that RFID will be adopted."[101] If Ashton is correct, legislation is required to ensure that the efficiencies of RFID technology continue to exist, while consumer privacy is protected. Since tort law claims for this technology are not effective, state laws covering RFIDs are inconsistent and inadequate, and the proposed federal regulations are flawed, ensuring that RFID use does not become ubiquitous before appropriate regulations are in place requires additional action.

¶36 Before the enactment of any RFID legislation, the effects of technology-specific legislation should be considered. With new technologies continually entering the market, adopting regulations that do not consider the future may have an ill effect on privacy protection for future surveillance technologies. RFIDs provide cost effective means to

---

[98] Eduardo Ustaran, *Data Protection and RFID Systems,* 3 PRIVACY & DATA PROTECTION 6, http://www.berwinleighton.com/download/PDP-RFIDtagsimplications.pdf; *see* Laurant, *supra* note 5 (quoting *Directive on Privacy and Electronic Communications*, OFFICIAL J. EUR. COMMUNITIES 37, July 12, 2002, http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf).
[99] Ustaran, *supra* note 98.
[100] *Id.* at 7.
[101] MANEY, *supra* note 4.

track items and people, but overly strict regulations can deter necessary RFID uses. Regulations that are too lenient, however, permit businesses to impinge on consumers' privacy rights.

¶37 Since the scope of RFID uses and potential costs are not certain at this time, it is crucial that RFID-specific legislation is avoided. Instead, legislation prohibiting the "underlying behavior" violating privacy principles should be adopted.[102] One effective way to address RFID legislation at the federal level is to amend various federal privacy laws as suggested by the Right to Know Act. Since the federal government has many broad privacy protection statutes, general amendments are a good approach. For example, the suggested amendment to Chapter 94-Privacy, of Title 15 of the U.S. Code creating an additional subchapter titled "AGGREGRATION OF NONPUBLIC PERSONAL INFORMATION AND RADIO FREQUENCY INDENTIFICATION INFORMATION" would protect collected information that is not intended to be public information. However, the words "Radio Frequency Identification" should not be included in order to avoid technology specific legislation. Included in this section should be prohibitions against all technologies that gather more information than is required to manage inventory. Additionally, as suggested by the Right to Know Act, the language in the amendment should prohibit disclosure of gathered information by electronic means to any third party.

¶38 The Electronic Communications Privacy Act (ECPA) also addresses the privacy of individuals.[103] The "act prohibits any person from intentionally intercepting, or endeavoring to intercept wire, oral or electronic communications by using an electronic, mechanical, or other device unless the conduct is specifically authorized or expressly not covered."[104] Although the current language of the act does not specifically cover RFID technology, small amendments to the act could encompass the mal-intended behaviors of retailers and third-parties.[105]

¶39 One of the paramount concerns to consumers is their lack of awareness that the products they purchase are equipped with RFID technology. Encompassed in the Wiretap Act[106] is the requirement that "anyone who intercepts electronic communication will be held in violation of the statute if proper consent has not been obtained."[107] Amending the

---

[102] Tavilla, *supra* note 21, at 15.
[103] 18 U.S.C. §§ 2510–2522 (2000); *see* Levary, *supra* note 96.
[104] Levary, *supra* note 96. *See* 18 U.S.C. §§ 2510–2522 (2000).
[105] *See* John Eden, *When Big Brother Privatizes: Commercial Surveillance, The Privacy Act of 1974, and the Future of RFID*, 2005 DUKE L. & TECH. REV. 0020 (2005), http://www.law.duke.edu/journals/dltr/articles/2005dltr0020.html.
[106] 18 U.S.C. § 2701 (2000); *see* Levary, *supra* note 96.
[107] 18 U.S.C. § 2701 (2000).

Wiretap Act so that RFID communications fall within the purview of electronic communications would suffice for the consent aspect of privacy protection from RFID tracking. This amendment would require businesses to obtain consent from consumers for RFID tracking. This need not be onerous for businesses or consumers. Obtaining consent could simply require a standard label on all items that have the ability to communicate information to consumers. By purchasing items with conspicuous labels the consumer is essentially consenting to information gathering[108] in the least restrictive way needed by the business to achieve reasonable goals.

¶40 Since violations of many current privacy statutes impose criminality on the violators, businesses have a strong incentive to remain within the boundaries imposed by these and similar regulations. If retailers and manufactures believe that RFIDs are important to their supply chains, they will follow broad privacy legislation.

CONCLUSION

¶41 Since "the RFID train is beginning to leave the station, . . . now is the right time to begin a national discussion about where, if at all, any lines will be drawn to protect privacy."[109] RFID technology provides many benefits for the retail and consumer products industries. As more time passes without the requisite legislation in place, consumers may lose the ability to protect their privacy from RFID tracking, or businesses may be faced with an unexpected halt to their RFID uses.

¶42 Individuals have a right to keep their private things, which include information not typically available to the naked eye, private. However, because intrusion upon seclusion, the typical conduit for privacy actions, is unable to protect individuals' privacy from RFID tracking by businesses, a new standard is required. State legislation is inadequate and implanting proposals from privacy advocates is unreasonable. This leaves federal legislation as the means of privacy protection. Amending existing federal privacy statutes, without enacting RFID-specific legislation, is the most effective alternative to control the "global blanket" of RFIDs.

---

[108] In this situation there is implied consent. "Implied consent is 'consent in fact' which is inferred 'from surrounding circumstances indicating that the party *knowingly agreed* to the surveillance.'" Williams v. Poulos 11 F.3d 271, 281 (1st Cir. 1993) (quoting United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987).

[109] Senator Patrick Leahy, Panel Discussion on Video Surveillance: Legal and Technological Challenges at Georgetown University Law Center (Mar. 23, 2004), *available* at http://www.spychips.com/alec-big-brother-barcode-article.html.