You Can Run, But You Can't Hide: Protecting Privacy from Radio Frequency Identification Technology

Jennifer E. Smith

Follow this and additional works at: http://scholarship.law.unc.edu/ncjolt

Part of the Law Commons

Recommended Citation
Available at: http://scholarship.law.unc.edu/ncjolt/vol8/iss2/3
YOU CAN RUN, BUT YOU CAN'T HIDE: PROTECTING PRIVACY FROM RADIO FREQUENCY IDENTIFICATION TECHNOLOGY

Jennifer E. Smith

RFID technology is a highly effective means of tracking products and people, and it is ready to be employed on a massive scale. Without regulation, RFID will be used to track both products and people. There is currently no government oversight of the use of RFID. Instead, the Federal Trade Commission allows companies that use RFID to self-regulate. Increasingly, RFID-tagged products are entering the stream of commerce without any notice to alert consumers to their presence. Moreover, with the development of miniscule tags, detection may become impossible unless labeling is mandated. In the absence of legislation, consumers may yet find recourse via federal or state unfair and deceptive trade practices law.

Radio frequency identification ("RFID") has been heralded as the next generation of bar codes, or perhaps more appropriately, "barcodes on steroids," because of its ability to efficiently track a product throughout the supply chain and beyond. RFID uses radio waves to identify products and people. In August 2006, Nike, in conjunction with Apple, launched a new product geared towards

---

1 J.D. Candidate, University of North Carolina School of Law, 2008. Special thanks to Professor Anne Klinefelter for her thoughtful guidance, my mother for her tireless support, and my father who loved to jog and first introduced me to privacy law.


runners: the Nike+ iPod Sport Kit. The $29 kit includes a nickel-sized sensor that may be placed in a Nike+ running shoe, which communicates with a receiver that attaches to an iPod nano using RFID. When the runner moves, the sensor in the shoe signals the receiver in the iPod, which allows the runner to monitor distance traveled, calories burned and speed achieved.

Scott Saponas, an avid runner and doctoral student at the University of Washington, was eager to purchase the Sport Kit. He soon realized, however, it could be used for non-athletic endeavors—like surreptitiously tracking the movement of others. With the aid of two other graduate students and a computer science professor, Saponas created several inexpensive RFID readers to detect the Nike sensors. From a remote location, they were able to detect anyone with a sensor who passed. Unfortunately, the Sport Kit packaging did not inform the runner that, as she tracks her athletic endeavors, others may be tracking her movements.

RFID technology is not the stuff of science fiction novels. It is here today and ready to be employed on a massive scale. Without regulation, RFID will be used to track both products and people. While some uses will undoubtedly be innovative, others have the potential to be nefarious. As such, consumers have a right to know if the product they purchased is RFID-tagged. This Recent Development discusses both current and future uses of RFID.

6 Iwasaki, supra note 4, at A1.
7 Id.
8 Id. Saponas and his fellow researchers posited several hypothetical scenarios, including how a (fictitious) obsessed ex-boyfriend could surreptitiously place the Nike transponder in the purse or other personal item of his ex-girlfriend and, with the help of a few strategically placed RFID readers, keep tabs on her whereabouts or stage "coincidental" meetings. Id.
9 Id.
10 Id.
11 Id.
Part I provides a brief background on privacy as it relates to the use of RFID technology. Part II discusses the privacy implications of widespread RFID use and the necessity of regulation. Part III is an analysis of recent efforts to regulate RFID use. Finally, Part IV concludes the inquiry by proposing and evaluating possible actions consumers can take to prevent lowered expectations and erosion of privacy resulting from the imminent widespread implementation of RFID systems.

I. THE RIGHT TO PRIVACY

A. Theoretical Underpinnings

The United States Constitution does not state an express right to privacy; however, the need to protect privacy has been debated for over a century. The modern American concept of privacy was first articulated in 1890 by Samuel D. Warren and Louis D. Brandeis in a *Harvard Law Review* article entitled "The Right to Privacy." Technological advances, such as the advent of photography and the popularity of tabloid journalism made intrusions into private life both easy and lucrative. In support of judicial recognition of a right to privacy, Warren and Brandeis noted:

> The design of the law must be to protect those persons with whose affairs the community has no legitimate concern, from being dragged into an undesirable and undesired publicity and to protect all persons, whatsoever; their position or station, from having matters which they may properly prefer to keep private, made public against their will. It is the unwarranted invasion of individual privacy which is reprehended, and to be, so far as possible, prevented.

For Warren and Brandeis, the threat to personal privacy posed by technological advances inspired their argument that individuals have a right "to be let alone." Subsequent case law led to a recognition of privacy-related torts and the development of a Constitutional basis for the analysis of certain privacy rights. The

---

13 Id. at 195–96.
14 Id. at 214–15.
15 Id. at 195 (citations omitted).
Fourth Amendment, in particular, has been interpreted to protect individuals from unreasonable invasions of privacy.

B. Case law

The right to privacy and technological advances often come into conflict. Technology used by the government in criminal investigations has been held to violate Fourth Amendment privacy rights. For example, Silverman v. United States involved the use of a "spike mike," a technologically advanced microphone placed by police in a heating duct to eavesdrop on an incriminating conversation. In Silverman, the Supreme Court expanded the reading of the Fourth Amendment and held that it "governs not only the seizure of tangible items, but extends as well to the recording of oral statements, overheard without any 'technical trespass under . . . local property law.'"

The notion that the Fourth Amendment protects private conversations was revisited in the landmark case of Katz v. United States, which also involved the intersection between technology and the right to privacy. In Katz, the government used a bug to overhear a suspect's telephone conversation in a public phone booth. The Court held that the Fourth Amendment protected individuals from government eavesdropping in a private conversation, despite the fact that the conversation took place within a public telephone booth. The Court reasoned that while the telephone booth was open to the public and located in a public

---

16 U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated; and no warrants shall issue but upon probable cause, supported by oath or affirmation and particularly describing the place to be searched and the persons or things to be seized.").
19 Id. at 506.
22 Id. at 348.
23 Id. at 352.
place, the act of shutting the door indicates an expectation that the conversation is private and free from government intrusion.\textsuperscript{24}

Although technological advances often raise privacy issues, not all technological innovations violate the right to privacy merely because they make it possible to track an individual’s movements. For example, in \textit{United States v. Knotts}\textsuperscript{25} the Supreme Court held that the Fourth Amendment does not apply to a “beeper,” a transmitting device that was technologically advanced at the time, used to track a person’s movements in public.\textsuperscript{26} The beeper in question was surreptitiously attached to a drum of chloroform that was transported in the defendant’s car. The Court noted that a person traveling on public highways “has no reasonable expectation of privacy in his movements from one place to another.”\textsuperscript{27} The Court explained that a beeper merely augmented the police’s ability to visually observe a subject in public.\textsuperscript{28} However, the Court specifically noted that the beeper was not used in any way to monitor movements once the chloroform was taken inside a private residence.\textsuperscript{29}

The line between tracking inside and outside of the home was more clearly defined in \textit{United States v. Karo}.\textsuperscript{30} In \textit{Karo}, the Court held that the government use of a beeper to monitor activity within a private home was a violation of the Fourth Amendment.\textsuperscript{31} Thus, while the Court has consistently protected private residences from unwarranted search, Fourth Amendment protection beyond the home is hardly guaranteed. The distinction between “in public” and “in the home” is often the determinative factor.

\textsuperscript{24} \textit{Id.}
\textsuperscript{25} 460 U.S. 276 (1983).
\textsuperscript{26} \textit{Id.} at 281–82.
\textsuperscript{27} \textit{Id.} at 281.
\textsuperscript{28} \textit{Id.} at 285.
\textsuperscript{29} \textit{Id.}
\textsuperscript{31} \textit{Id.} at 714 (holding that a beeper placed on a can of ether and used to monitor movement within a private residence violated respondents’ Fourth Amendment expectation of privacy in a private residence).
In State v. Jackson, a technologically updated variation of Knotts, the Washington Supreme Court considered the constitutionality of the police planting a Global Positioning System ("GPS") in a vehicle to remotely track its location. The court held that the police needed a warrant in order to attach a GPS device to a car. In reaching its conclusion, the court noted that the content of the information gathered could reveal information about a person’s "preferences, alignments, associations, personal ills, or foibles." It is important to note that all the above cases involved government surveillance in some form. In United States v. Jacobsen, the Supreme Court made clear that when private information is collected by a non-government entity, the government’s subsequent use of the information is not a violation of the Fourth Amendment. The Court noted, "[o]nce frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information."

The implications of this ruling are particularly troubling in the context of RFID. RFID is on the cusp of widespread implementation because it is a highly effective means of tracking products. Scholars forecast that in the near future all people will carry commercial or state issued products that are RFID-tagged. Thus, RFID is not just a highly effective means of tracking products; it is also a highly effective means of tracking people. As the ruling in Jacobsen makes clear, once information has been compiled by non-government entities, it can be accessed by corporations or individuals with financial resources who can buy

---

32 76 P.3d 217 (Wash. 2003).
33 Id. at 224.
34 Id. at 223.
36 Id. at 115 (holding that government sampling of the contents of a package opened by a third party did not violate the Fourth Amendment).
37 Id. at 117.
the information, hackers who can steal the information, and/or the government which could subpoena the information. Unless consumers take action now, our identity, whereabouts, preferences, and peculiarities will soon be more easily traceable by corporations, hackers, and the government.

C. What is RFID?

An RFID system has two components: (1) an RFID tag or transponder, which includes a microchip attached to an antenna; and (2) a reader, which translates radio waves reflected from the RFID tag into digital information that can, in turn, be passed on to computers. The reader emits "electromagnetic waves." The tag antenna is tuned to receive these waves. An RFID tag may be either passive or active. A passive tag draws power from a nearby reader, while an active tag, usually powered by a battery, continuously emits information until the power source expires. RFIDs average a few square centimeters in size, but some are miniscule. Hitachi has designed an RFID tag measuring just 0.05 mm by 0.05 mm, which it plans to market by 2010. The tiny tag, which is smaller than a grain of sand, may be easily incorporated into paper and currency.

RFID may be used as an alternative or supplement to barcodes. Unlike products with a bar code, which must individually pass within the line of sight of a reader, multiple RFID-tagged products may be scanned when they come within range of a reader. For example, a truck carrying new inventory would have to be

---

39 RFID FAQs, supra note 3.
41 Id.
42 Id.
44 Id.
unloaded and reloaded to scan each box with a bar code; but, if the products are RFID-tagged, the contents of the truck could be almost instantaneously tallied if driven past an RFID reader.46

Perhaps the most important feature of an RFID tag is its uniqueness. Unlike bar codes that employ the Universal Product Code ("UPC"), by which identical products share the same bar code, RFID employs the Electronic Product Code ("EPC"), which gives each and every product a unique identification.47 For example, whereas a can of Coca-Cola with a UPC would be indistinguishable from any other can of Coca-Cola, a can of Coca-Cola with an EPC is unique and distinguishable from every other one in the world.48 Since EPC uses a ninety-six-bit code, which allows "eighty thousand trillion trillion" objects to each be assigned a unique number, there will be no shortage of numbers available for identification and tracking purposes.49

The majority of consumers are unaware of the presence of RFID in products already sold.50 Currently, no laws or regulations require the government, retailers, or manufacturers to disclose to consumers that the product they carry is tagged with a unique code. As RFID tags become smaller and smaller, it will be very difficult, if not impossible, for even the savviest of consumers to detect a tag unless regulation is passed requiring both proper labeling and a means of deactivating the tag. Failure to take action now will result in tagging and potential tracking on a massive scale.


48 Id.


II. USES OF RFID

A. The Race Begins: Current Uses of RFID

Perhaps one of the most visible uses of RFID occurs at tollbooths across the nation. Motorists on I-95 who utilize the E-Z Pass system, which allows a vehicle to pass through a toll without stopping, is made possible by an RFID tag, usually attached to the vehicle’s windshield, which is scanned by a reader at the toll booth. While many motorists are happy to save time, they may not realize that their travels are documented. E-Z Pass records have played a key role in criminal and civil litigation. In fact, “investigators in criminal investigations already regularly subpoena E-Z Pass toll records, which come from RFID records, to figure out where an individual’s car was at a particular time.”1 RFID-enabled toll records have also been used to draw inferences about motorists’ character. In an Illinois child custody battle, the husband’s attorney subpoenaed the wife’s I-Pass toll records to show she often worked late, supporting an inference that she was not spending time with the children.2

Another major use for RFID is in retail. In 2005, Wal-Mart required its one hundred top suppliers to equip their products with RFID tags and required two hundred more suppliers to tag their products in 2006.3 But Wal-Mart had already surreptitiously tested RFID on its customers without their knowledge. Over the course of four months in 2003, Wal-Mart, in conjunction with Procter and Gamble, placed RFID tags on Max Factor Lipfinity lipstick packages in an Oklahoma store.4 Without the customers’ knowledge, RFID tags were attached to the lipstick, which triggered a video monitor whenever the product was taken off the

---


2 ALBRECHT & MCINTYRE, supra note 47, at 139.


shelf, allowing Procter and Gamble product analysts over seven hundred miles away to observe how the customers handled the lipstick from the moment they took it off the shelf.\textsuperscript{55} Despite the negative publicity generated by the secret Lipfinity study, other major American retailers, including Target and Albertson’s, have announced plans to tag their products with RFID.\textsuperscript{56}

Around the globe, department stores are gearing up to implement RFID. During a four-month test period using RFID on women’s shoes at Mitsukoshi Department Stores in Japan, sales associates were given instant access to the RFID-tagged inventory, via handheld PDAs.\textsuperscript{57} Consequently, trips to the stock room were decreased by twenty-five percent, and sales associates doubled the amount of product shown while decreasing customer wait time.\textsuperscript{58} Sales rose 10.3\% during the trial.\textsuperscript{59}

Retailers are not the only ones excited about the potential for RFID systems. Several libraries (though no law libraries to date) are using RFID tags on books to simplify the management of library collections.\textsuperscript{60} By using an RFID scanner, library personnel can quickly determine if a book is missing or out of place. The checkout process is also expedited because a stack of books can be scanned simultaneously, instead of one by one.\textsuperscript{61} The Chicago State University library has recently tagged all of its books, CDs, and DVDs with an RFID chip.\textsuperscript{62}

RFID has been used not just to track products, but also as an integral component of the product, from toys\textsuperscript{63} to automobiles\textsuperscript{64} to

\textsuperscript{55} Id.
\textsuperscript{56} Hildner, supra note 53, at 134.
\textsuperscript{57} Power, supra note 2, at 14.
\textsuperscript{58} Id.
\textsuperscript{59} Id.
\textsuperscript{60} See Dan Harmon, AALL Spectrum, LAWYER’S PC, Dec. 15, 2006.
\textsuperscript{61} Id. From personal experience working at a circulation desk, I can attest that this can be a lengthy process, particularly when a patron wishes to renew several books.
\textsuperscript{63} Seth Schiesel, It's a Game, It's a Toy, It's Mattel's Big Gamble, N.Y. TIMES, July 20, 2006, at E1. Mattel is using RFID in its new game, HyperScan.
Protecting Privacy from RFID

However, the use of RFID-tagged products raises serious privacy concerns. One of the most troubling uses relates to credit cards. Major credit card companies, including Visa, MasterCard, and American Express, have issued tens of millions of cards using RFID, forgoing the need for a signature or physical swiping through a machine. The credit card companies have marketed the cards as secure by means of encryption, but researchers Tom Heydt-Benjamin and Kevin Fu cobbled together an inexpensive RFID reader using readily available computer and radio components and found that the cardholder's name and other data could be read in plain text. Information on the cards could be read through wallets, clothing, and envelopes. While the distance at which a card could be read ranges from a few inches to several feet, the researchers demonstrated that "even the shortest distance could allow a would-be card skimmer to mill about in a crowded place and pull data from the wallets of passersby, or to collect data from envelopes sitting in mailboxes." HyperScan is a video game and collectible card hybrid in which players battle by swiping RFID-tagged cards over the HyperScan reader and then duking it out on-screen.

64 Raymund Flandez, *Reinventing the Wheel: The Latest Car Technology*, WALL ST. J., Nov. 2, 2006, at D4. SmarTire Systems Inc. uses RFID technology to provide real-time pressure readings. The RFID-tagged tires send pressure and temperature readings to a receiver, which displays the information to the driver.

65 Mark Baard, *Afraid Accessories from Belfast*, BOSTON GLOBE, Oct. 16, 2006, at D2. A Belfast designer created an RFID-tagged bracelet that communicates with its jewelry box. The jewelry box lights up when the bracelet is taken out and changes colors, depending on the length of time it remains out of the box and the number of times worn.


67 Id.

68 Id.

69 Id. See also Jennifer Granick, *Patently Bad Move Gags Critics*, WIRED, Feb. 28, 2007, http://www.wired.com/news/columns/0,72819-0.html (on file with the North Carolina Journal of Law & Technology). Researchers' ability to experiment with RFID and showcase its vulnerabilities may be conscribed. In February, HID Global, a company that holds patents for RFID access-control devices, threatened to sue a researcher who planned to demonstrate a technique for cloning RFID proximity cards.
Another source of personal information ripe for abuse is passports. Beginning January 1, 2007, all passports issued by the U.S. State Department contain an active RFID chip embedded in them. The RFID tag embedded in each passport contains the name, nationality, date of birth, and digitized photograph of the traveler. Given the ease with which an inexpensive RFID reader can be made, the new passports create health and safety risks for Americans traveling abroad who could be targeted for theft or kidnapping. Moreover, the REAL ID Act of 2005 requires anyone who travels domestically by airplane to have a state-issued ID that complies with the Act's standards. Incorporating an RFID chip into drivers' licenses is a likely next step.

RFID is already used to track people. Not surprisingly, the first human guinea pigs have been vulnerable populations of refugees, indigent patients, and children. In 1994, in conjunction with Operation Sea Signal, the U.S. government used RFID-tagged bracelets to track fifty thousand Haitian and Cuban refugees who were fleeing their native countries. Anyone who removed the bracelet was sent to a detention facility. In the past few years, United States citizens have also served as test subjects in human RFID trials. For example, in 2004, the Robert Woods Johnson Foundation funded a three-month trial using RFID tags on indigent patients at The Elvis Presley Memorial Trauma Center. Each patient entering the emergency room was tagged with an RFID

---

71 Id.
72 For this reason, Wired Magazine recommended hitting the passport with a hammer to disable the chip, but cautioned that tampering with a passport is punishable by up to twenty-five years in prison. Jenna Worthman, How To: Disable RFID in Your New Passport, WIRED, Jan. 2007, http://www.wired.com/wired/archive/15.01/start.html?pg=9 (on file with the North Carolina Journal of Law & Technology).
74 ALBRECHT & MCINTYRE, supra note 47, at 168–69.
75 Id.
anklet so that he could be tracked by one of the twenty-five readers installed throughout the hospital.  

Children have also been the unwitting targets of RFID tagging. In January 2005, Britain Elementary School in California required all students to wear RFID-tagged cards on lanyards around their necks and installed readers at the entrance of classrooms and certain bathrooms. The school entered an agreement with InCom, the maker of InClass RFID systems, that allowed the company to test the RFID system on the school’s students in exchange for a donation. However, neither students nor parents were informed that the student cards were RFID-tagged. Parents protested and readers above bathrooms were removed, but the school maintained that the cards were useful for determining accurate attendance and threatened disciplinary action if students did not wear them.

The RFID tags discussed in these studies were all worn outside the body and could be removed. However, subdermal chips have gained popularity for tracking pets. The “HomeAgain” chip has already been implanted into thousands of dogs and cats. But wandering Labradors and wayward Abyssinians now have human company. In 2006, CityWatcher.com, a private video surveillance company, embedded the “VeriChip,” a glass encapsulated RFID tag, into two of its employees. The company said it was “testing the technology as a way of controlling access to a room where it holds security video footage for government agencies and the

77 Id.
79 Id.
80 Id.
81 Id.
police.” Human implantation gives rise to a bevy of concerns, including the conditions under which employee consent is granted, the health risks of de-chipping, and the possibility of monitoring employees’ off-duty conduct.85

B. Run for Your Life: Future Uses of RFID

Some of the proposed uses for RFID are commonsensical, like using RFID tags to curtail pharmaceutical counterfeiting86 and tracking baggage at the airport.87 In contrast, other potential uses of RFID are fantastical, like RFID-tagged clothing that communicates with a washing machine to tell it the temperature at which it should be washed, or a microwave that can “read the tags on packages and cook the food without explicit instructions, or refrigerators that can recognize expired foodstuffs, and closets that can tally their contents.”88

Other proposed future uses for RFID raise privacy concerns. Since RFID technology is still in its nascent stages, few of these applications have made it to the commercial market. However, a review of patent applications for products that incorporate RFID provides a glimpse at products currently being readied for consumption. Many of these patent applications raise potential privacy concerns. For example, in 2003, BellSouth bought rights

84 Id.
85 Recognizing the possibility of employee coercion, Wisconsin Governor Jim Doyle signed a bill that makes it illegal to require an employee to be implanted. Wisconsin Bars Forced Implantation of Microchips, 5 PRIV. & SEC. L. REP. 812 (2006).
86 Pharmaceutical counterfeiting is an estimated $512 billion industry. Counterfeiting is of particular concern to the pharmaceutical industry because imposter drugs can, at best, have no effect, and at worst cause death or serious illness. See generally Maria Nelson, Michelle Vizurraga & David Change, Counterfeit Pharmaceuticals: A Worldwide Problem, 96 TRADEMARK REP. 1068 (2006).
87 Airlines spend $2.5 billion annually to find and return the thirty million bags mishandled each year. RFID technology would allow airlines to locate a bag if it did not make the proper airplane and to alert passengers early, saving them the time and aggravation of waiting at the baggage carousel. Jeff Bailey, Frustration Grows at Carousel As More Baggage Goes Astray, N.Y. TIMES, Nov. 12, 2006, at 11.
88 Hildner, supra note 53, at 136.
to a patent entitled “Radio-frequency tags for sorting post-consumer items,” which outlines a plan to compile and sell data on consumers’ trash. According to the application, “[i]nformation concerning a post-consumption item may be linked (by serial number, for example) with information concerning the pre-consumed item collected by other data collection systems.” By combining captured pre-consumer information with post-consumption information, “the entire life cycle of an item may be tracked.” This information may be useful to any number of entities, including retailers, manufacturers, distributors, and the like. This application demonstrates that businesses are not only interested in tracking a product throughout the supply chain, but also want to monitor how that product is being used when it is taken home.

While BellSouth wants to track consumers through their trash, IBM took a more direct approach. In 2002, IBM developers filed a patent application entitled “Identification and tracking of persons using RFID-tagged items.” The application details how RFID tags, each with a unique identification number, can be used to infer demographic information about the individual. Next, the application explains how information may be stored and a more detailed picture compiled with each purchase until the exact identity of a person may be ascertained, at which point the “person

90 Id.
91 Id.
92 Id.
94 Id.

[S]ome characteristics such as demographics (e.g. age, race, sex, etc.) about the person may be determined based on certain predetermined statistical information. For example, if items that are carried on the person are highly expensive name brands, e.g. Rolex watch, then the person may be classified in the upper-middle class income bracket. In another example, if the items that are carried on the person are “female” items typically associated with women, e.g. a purse, scarf, pantyhose, then the gender of the person can be determined as female.

Id.
tracking unit" assigns and stores the identity of the person and his associated goods. Finally, while the "person tracking unit" is described in the context of a retail store, the application states that it can be used to track people in other areas, including "shopping malls, airports, train stations, bus stations, elevators, trains, airplanes, restroom, sports arenas, libraries, theaters, museums, etc." If IBM or another business goes forward with a similar system for tracking people, our every movement could be tracked.

Anticipating widespread RFID implementation, IBM has already created the "Margaret Program." Named for the program developer's wealthy mother-in-law, the "Margaret Program" would allow employees and sales associates to give preferential treatment to affluent customers the moment they walk in the door. If IBM or another business goes forward with a similar system for tracking people, our every movement could be tracked.

Uses of RFID, like the "Margaret Program," exemplify how RFID technology may be used by companies to discriminate quickly among customers and provide preferential treatment.

Expanding on the preferential treatment theme, the RFID Journal recommends, "[t]he same system could be used in upscale restaurants or retail boutiques, where a high degree of personal

---

95 Id.

Once the exact identity or some demographics or other characteristics of the person have been determined, the person tracking unit relies on this information to track the person as the person moves through the roaming areas. The person tracking unit may assign a tracking number to each identified person and store the tracking number in association with the collection of RFID-tagged product information.

96 Id.


98 Id.
service is important.\textsuperscript{99} The widespread presence of anti-theft portals will expedite IBM's plans. In 2004, Checkpoint, the largest retailer of anti-theft devices, announced plans to purchase one hundred million RFID tags for use in commerce.\textsuperscript{100} The prevalence of anti-theft portals, which may be easily converted to RFID portals, means that people carrying RFID-tagged items can be "electronically frisked" wherever they go, without their knowledge or consent.\textsuperscript{101}

Finally, RFID can be used specifically for the purpose of tracking the location of particular individuals. As noted above, one American company has already injected its employees with the VeriChip, which is generally injected into the bicep.\textsuperscript{102} Persephone, a California company, has taken injection to the next level. They filed a patent application entitled "Method and Apparatus for Locating and Tracking Persons," which proposes implantation in the head, torso, deep muscle of limbs, the gastrointestinal tract, and uterus.\textsuperscript{103} These locations within the body were specifically selected to decrease the possibility of removal of the RFID chip. The application suggests the implant could be used to track runaways, kidnapping victims, inmates, military personnel, mentally impaired individuals, and even business travelers.\textsuperscript{104} However, the application fails to consider the potentially gruesome consequences of removing a chip—either with or without the implanted person’s consent. The ramifications of RFID implants imply that people could be tracked anywhere, anytime—in both public and private places.

\textsuperscript{100}Id.
\textsuperscript{101}ALBRECHT & MCINTYRE, supra note 47, at 5.
\textsuperscript{102}Waters, supra note 83.
\textsuperscript{104}Id.
III. PAST REGULATORY ATTEMPTS

There is currently no government oversight of the use of RFID. Instead, the Federal Trade Commission (FTC) allows companies that use RFID to self-regulate. While the Fair Industry Practices ("FIPs") state that businesses should disclose product information to consumers, the FIPs are recommendations and do not have the effect of law. Increasingly, RFID-tagged products are entering the stream of commerce without any notice to alert consumers to their presence; moreover, with the development of miniscule tags, detection may be impossible in the absence of labeling.

RFID advocates want to maintain the status quo, which gives manufacturers and retailers free reign. In support of an unregulated RFID industry, the Progressive Policy Institute stated, "[c]onsumers will get used to RFID technology over time and will develop appropriate expectations about the level of privacy they have in stores." Thus far, both federal and state attempts to regulate RFID have been unsuccessful. On the federal level, Representative Gerald Kleczka introduced the "Opt Out of ID Chips Act" in June 2004. The proposed legislation required businesses to label all products that contained an RFID tag and provide the purchaser with the option of having the tag removed or permanently disabled at the time of sale. That same year, the General Services Administration, a government agency that supports the functioning of federal agencies, issued a bulletin directing federal agency administrators "to consider action that can be taken to advance the [RFID] industry by demonstrating the long-term intent of the

106 See Samiljan, supra note 43.
agency to adopt RFID technological solutions." In the spring of 2005, the Senate Republican High Tech Task Force identified RFID as a new technology that should be protected from "premature regulation or legislation." The report also noted, "RFID holds tremendous promise for our economy, including military logistics and commercial inventory efficiencies, and should not be saddled prematurely with regulation." As a result of this opposition, the "Opt Out of ID Chips Act" did not make it out of committee.

State regulation has also failed. Legislation regulating RFID use has been introduced in nine states. While several drew broad support initially, each proposal was defeated when RFID industry representatives became involved and lobbied against the legislation. However, another bill will soon be introduced in Virginia. In January 2007, Albert C. Eisenberg pre-filed H.B. 2086, which would require businesses to notify consumers if a product contains RFID. Passage of the Virginia bill could spur introduction of similar bills in other states and at the federal level.

112 Id.
114 Id.
IV. SOLUTIONS FOR TODAY

In the absence of legislation, consumers may find recourse under federal or state unfair and deceptive trade practice law. Under section 5 of the Federal Trade Commission Act, consumers could have a cause of action against businesses who fail to notify consumers that a product contains RFID. The Act applies to advertisements as well as labels. Moreover, courts insist on a higher degree of truth in labeling, as compared with advertising, because consumers are more apt to accept labeling statements literally.

Consumers may also have a cause of action at the state level based on unfair and deceptive trade practices. The majority of states have enacted legislation with language that closely tracks the federal act. Furthermore, statutes establishing a cause of action for unfair and deceptive trade practice acts have already served as the basis for redress from other new technologies that intrude on privacy. In 2002, Connecticut's consumer protection agency filed


Unfair methods of competition unlawful; prevention by Commission
(a) Declaration of unlawfulness; power to prohibit unfair practices; inapplicability to foreign trade.

(1) Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.

(2) The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations, except banks, savings and loan institutions described in section 18(f)(3), Federal credit unions described in section 18(f)(4), common carriers subject to the Acts to regulate commerce, air carriers and foreign air carriers subject to the Federal Aviation Act of 1958, and persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act, 1921, as amended, except as provided in section 406(b) of said Act, from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.

Id.


a complaint alleging violation of the state’s Unfair Trade Practices Act against a rental car agency that used the rental car’s GPS device to charge a fee to customers who drove above the set speed limit.\textsuperscript{120} In the resulting lawsuit, the Connecticut Supreme Court held that the fee was an illegal penalty that violated the Connecticut Unfair Trade Practices Act.\textsuperscript{121} To protect consumers from rental agency spying and fee-charging, California\textsuperscript{122} and New York\textsuperscript{123} passed bills prohibiting the use of GPS to impose rental fees. State Senator Charles Fuschillo, the New York bill’s author, stated, “[w]hen you rent a car from a company, you should not have to worry that your every move is being monitored or that you are always under suspicion. . . . The mere fact that technology enables a company to do so does not mandate that privacy be invaded.”\textsuperscript{124}

In the context of RFID, a consumer, a class of consumers, or the state attorney general could bring a suit against a business that failed to properly label products with RFID tags or provided intentionally misleading labels. For example, as noted above, the literature accompanying the Nike+ iPod Sport Kit advises users to “just drop the sensor in their Nike+ shoes and forget about it,” despite the fact that the sensor has an on-off switch.\textsuperscript{125} This kind of information does not inform but rather lulls consumers into a false sense of security. Under many state deceptive practices statutes, a consumer could argue that this language misleads the consumer and increases the likelihood that a runner will leave the sensor in active mode at all times. Similarly, in response to the public outcry resulting from the uncovering of the secret Lipfinity study, Wal-Mart introduced “shelf-talkers,” tear-off leaflets similar to those found bearing coupons in many grocery store aisles. The

\textsuperscript{120} Am. Car Rental Inc. v. Comm’r of Consumer Prot., 868 A.2d 1198, 1201 (Conn. 2005).
\textsuperscript{121} Id. at 1200; see also Connecticut Unfair Trade Practices Act, C.G.S. § 42-110a (2004).
\textsuperscript{123} H.R. 2588, 227th Leg. (N.Y. 2004).
\textsuperscript{124} Electronic Surveillance: New York Bars Use of GPS to Charge Fees to Car Renters Over Speeding, Location, 3 PRIV. & SEC. L. REP. 1274 (2004).
\textsuperscript{125} Iwasaki, supra note 4, at A12.
“shelf-talkers” notify consumers that some products are RFID-tagged. However, the leaflet does not identify which products are tagged or how to deactivate a tag, but rather focuses on the benefits of RFID. A consumer could argue that the shelf-talker creates confusion and misunderstanding and provides little useful information about RFID-tagged products.

Consumers who use RFID-enabled credit cards could have a cause of action based on unfair trade practice and state data breach notification laws. Data breach laws, which have been enacted in thirty-four states with the goal of preventing identity theft, require businesses to notify consumers if their credit card information has been compromised. For instance, in In Re BJ’s Wholesale Club, the FTC alleged that a company’s failure to ensure adequate security measures constituted an unfair practice. As noted above, researchers have already shown the vulnerability of credit cards that use RFID. Using an argument similar to that in BJ’s, consumers could argue that the inadequate security measures used to encrypt RFID credit cards, coupled with the fact that these vulnerabilities have been well-documented by researchers, should be deemed an unfair practice.

---

126 Hildner, supra note 53, at 165.
127 Id.
131 Id.
132 Schwartz, supra note 66, at C1.
V. CONCLUSION

RFID is no longer the technology of the future. Mass distribution of RFID-tagged products is imminent. Like the Nike+ iPod Sport Kit, products are sold each day with RFID tags and the vast majority of consumers are unaware of what RFID is, let alone that the products they buy may be RFID-tagged. Consumers cannot object to that which they do not know. The ability to track a person's belongings, like shoes, keys, or a wallet, allows third parties—including corporations and identity thieves—to track the person.

The things we carry reveal information about our lifestyle, habits, and preferences. Once this information is compiled by commercial entities, it may be sold or used by others, including the government. As the current and future uses of RFID demonstrate, technology can be introduced for one purpose, such as increasing visibility of a product in the supply chain, but evolve to permit other uses, like sub-dermal implants used to track our actions wherever we go. In the absence of regulation, consumers should protect their privacy by seeking recourse through federal or state unfair or deceptive trade practice laws. Consumers must stand up for their rights or risk losing the race.