I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

LAURA M. ULATOWSKI [*]

Recent Developments in RFID Technology: Weighing Utility Against Potential Privacy Concerns

Abstract: Radio Frequency Identification ("RFIDs") devices are simple, technologically advanced labels. These bar codes of the future hold the potential to label and track everything from inventory to credit cards to animals to humans, all at a low cost. As the price of RFIDs and their associated data analysis has fallen, RFIDs have become ubiquitous throughout American society. They will promote security, protect patient safety, improve inventory management and expedite transactions. However, some privacy advocates still fear that the government and private industries will use RFIDs to track and monitor American citizens and misuse their personal information. This article provides an update on developments in RFID technology since 2005.

[*] Laura M. Ulatowski is a 2008 Juris Doctor candidate at The Ohio State University Michael E. Moritz College of Law. She earned a Bachelor of Science: Engineering, *magna cum laude*, as well as a Master of Science: Engineering, in biomedical engineering from Case Western Reserve University. The author would like to thank Katy K. Liu, a 2007 graduate of the Ohio State University Michael E. Moritz College of Law.

I. INTRODUCTION

Radio Frequency Identification ("RFID") devices have proliferated through many aspects of life in the last several years.[1] These small devices have the potential to "provide security, improve inventory management and [expedite] everyday transactions."[2] For example, some hospitals employ RFID tags in newborn nurseries to guard babies against "kidnapping or accidental switching."[3] Libraries use RFID tags to prevent theft and increase efficiency.[4] Additionally, many pet owners "microchip" dogs and cats with RFID chips so that lost pets can be easily identified and returned.[5] Farmers and researchers also utilize RFID tags to identify animals and to track food-borne diseases.[6] Retailers use RFID technology to gain supply chain visibility, which improves product inventory accuracy and

[1] This note covers the post-2005 advances in RFID technology. For a review of the state of RFID technology pre-2005, *see* Katherine Delaney, Note, *2004 RFID: Privacy Year in Review: America's Privacy Laws Fall Short with RFID Regulation*, 1 ISJLP 543, 544 (2005). For a complete review of RFID uses, policy and associated law, *see* Jonathan Weinberg, *Tracking RFID*, 3 ISJLP 777 (2007–08).

[2] RFID and Privacy–A Public Information Center, Why is RFID Important?, http://rfidprivacy.mit.edu/access/why.html (last visited Jan. 20, 2008); *see* Francoise Gilbert, *No Place to Hide? Compliance and Contractual Issues in the Use of Location-Aware Technologies*, 11 No. 2 J. INTERNET L. 3, 4–5 (2007); *see generally* Benjamin Burnham, Comment, *Hitching a Ride: Every Time You Take a Drive, the Government is Riding with You*, 39 J. MARSHALL L. REV. 1499 (2005–2006).

[3] *See* Jeff Aldridge, *"Total Security Solution" Thwarts Infant Abduction from Charlotte Hospital*, INFANT SEC. NEWS, August 2005, http://www.saione.com/Newsletters/ISN/ISN08.doc; *but see* Crystal Spivey, *Breathing New Life into HIPAA's UHID–Is the FDA's Green Light to the Verichip^{TM} the Prince Charming Sleeping Beauty has been Waiting for?*, 9 DEPAUL J. HEALTH CARE L. 1317 (2005–06).

[4] *See* American Library Association, RFID in Libraries: Privacy and Confidentiality Guidelines, http://www.ala.org/ala/oif/statementspols/otherpolicies/rfidinlibraries.pdf (last visited Jan. 20, 2008).

[5] *See, e.g.*, Pet-ID, Microchip Information, http://www.pet-id.net/whatispetid.htm (last visited Jan. 20, 2008).

[6] RFID and Privacy, *supra* note 2; *see also* Jackson W. Adams, Comment, *Cow 54, Where are You? Producer Liability and the National Animal Identification System*, 23 J. CONTEMP. HEALTH LAW & POL'Y 106 (2006–07) (discussing the National Animal Identification System).

allows retailers to keep popular items on store shelves.[7] Even drug companies and pharmacies are beginning to use RFID devices in order to stop counterfeit pharmaceuticals from entering the drug supply chain.[8] RFID chips also have incredible potential for use in implantable medical devices.[9] Student identification cards, parking garage entrance cards, apartment keys, and employee badges all use RFID technologies; furthermore, the government now uses RFID tags in U.S. passports and has considered them for many other purposes.[10]

RFID technology is not new, but tags have never been used as widely as they are today because they have been prohibitively expensive. With the recent significant reduction in the price of both making the chip and analyzing the associated data, both the government and private industry seem to be jumping on the RFID bandwagon.[11] While RFID devices promise exciting technological advancements that will make life easier for the average American,

[7] IBM, RFID for Supply Chain Management and In-Store Operations from IBM, http://www-03.ibm.com/industries/consumerproducts/doc/content/solution/956491123.html (last visited Jan. 20, 2008).

[8] RFID and Privacy, *supra* note 2; *see, e.g.*, Suchira Ghosh, Note, *The R.F.I.D. Act of 2006 and E-Pedigrees: Tackling the Problem of Counterfeit Drugs in the United States Wholesale Industry*, 13 MICH. TELECOMM. & TECH. L. REV. 577 (2007).

[9] RFIDs have potential applications in cardiac monitoring, seizure disorder monitoring and treatment, blood glucose monitoring, infant and pediatric thermometry and sleep apnea monitoring, continuous blood pressure monitoring and patient, caregiver and equipment identification, location and verification. *See* Frederick G. Weiss, Sensors: Implications of RFIDs for Medical Instrumentation, http://www.devicelink.com/mem/archive/00/10/006.html (last visited Jan. 20, 2008).

[10] Nicole A. Ozer, *Rights "Chipped" Away: RFID and Identification Documents* 2 (Draft 2007), *available at* http://stlr.stanford.edu/pdf/Ozer-RightsChippedAway.pdf/.

[11] While no federal or state laws protect the information gathered using RFIDs, several states have enacted statutes that give consumers minimal protection from RFIDs. *See* Matt Hamblen, *Privacy Concerns Dog IT Efforts to Implement RFID*, COMPUTERWORLD, Oct. 15, 2007, http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=305197&taxonomyId=17&intsrc=kc_top ("Wisconsin and Idaho have passed laws prohibiting the implantation of RFID chips in people without their consent . . . [and] five more states are debating similar measures . . . California [has a law] requiring businesses to notify consumers that a product has a tag."); *see also* Renee Boucher Ferguson, *California Law Bans Forced Human RFID Tagging*, EWEEK.COM, Oct. 15, 2007, http://www.eweek.com/article2/0,1895,2198130,00.asp.

some opponents fear that RFID tags will have a detrimental impact on personal privacy.[12]

Many people fear that RFID devices have the potential to chronicle each person's daily activities, effectively rendering anonymity a thing of the past.[13] However, in a post-9/11 world, with RFID tags' promise of enhanced safety and security, most citizens seem to have become more willing to surrender their privacy in exchange for helping police officers and intelligence agencies stop terrorists. The government and private sector, however, must be aware of the fact that these RFID chips have the potential to leak private information without a person's consent to anyone with an RFID reader. So those with the power to develop RFID policy must weigh the threats to privacy inherent in RFID technology against the efficiency these chips provide and the potential aid this tracking technology could give to law enforcement and intelligence agencies in their mission to protect public safety.

Both federal and state attempts to regulate RFID chips in the retail context have been largely unsuccessful.[14] RFID proponents have advocated strongly in favor of maintaining the status quo of government inaction.[15] Some RFID professionals believe that government action could stall the development of RFID technology and would amount to nothing more than "lawmakers overreact[ing] to security and privacy concerns by legislating the technology."[16]

Current RFID technology does not have the ability to protect data confidentiality, but since engineers have not yet developed the best way to improve security in the tags, the government should not yet legislate and rob developers of their ability to engineer an appropriate

[12] Delaney, *supra* note 1, at 543; *contra.* Gary Hartley, *Opinion: The RFID Tag Threat is Overrated*, COMPUTERWORLD N.Z., Sept. 19, 2007, http://computerworld.co.nz/news.nsf/news/06F345DFA23BF45BCC257356000F1D0D.

[13] Andrew Askland, *What, Me Worry? The Multi-Front Assault on Privacy*, 25 ST. LOUIS U. PUB. L. REV. 33, 44 (2006).

[14] Jennifer E. Smith, *You Can Run, but You Can't Hide: Protecting Privacy from Radio Frequency Identification Technology*, 8 N.C. J. L. & TECH. 249, 266 (2007); *see generally* Posting by RFIDblogger to RFID Law Blog by McKenna Long & Aldridge LLP, http://rfidlawblog.mckennalong.com/archives/cat-state-legislation.html (Sept. 6, 2007).

[15] Smith, *supra* note 14, at 266.

[16] Robert Westervelt, *RSA Panel Says Privacy Legislation too Premature for RFID*, SEARCHSECURITY.COM, Feb. 7, 2007, http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1242602,00.html.

solution.[17] Instead of the government legislating technology, developers should be able to determine the most cost-effective, elegant solution without legislative hurdles to overcome. One retail industry work group has released guidelines for RFID use under the guidance of the Center for Democracy and Technology "to provide guidance for policymakers, developers and users about privacy in the context of RFID technology."[18]

These guidelines might be the ideal way to regulate RFID's emerging technology. With proper privacy consideration, RFID technology should have the freedom to reach its lofty goals: aiding economics, efficiency and safety in many areas. This note examines recent developments in RFID technology. Part II discusses the simplicity of RFID technology and why these "bar codes on steroids"[19] are more popular now than ever before. Part III reviews new and newly considered RFID uses in both the private sector and the government, examining the privacy threats associated with each use.

II. TODAY'S RFIDS: SMALLER, CHEAPER AND MORE POWERFUL THAN EVER BEFORE

RFID technology's profound tracking capabilities are wrapped up in a compact design. An RFID tag comprises a computer microchip with a small amount of memory, which is encased in a protective covering and coupled with a miniature antenna.[20] Each antenna transmits its signal via radio frequency waves to an RFID reader, which converts the radio waves to a digital signal that can be sent to a computer for further processing and tracking.[21]

[17] *Id.* (quoting Ari Juels, principal research scientist at RSA Laboratories).

[18] Center for Democracy & Technology, *CDT Working Group on RFID: Privacy Best Practices for Deployment of RFID Technology* (Interim Draft May 1, 2006), http://www.cdt.org/privacy/20060501rfid-best-practices.php.

[19] Smith, *supra* note 14, at 249.

[20] John M. Eden, Note, *When Big Brother Privatizes: Commercial Surveillance, the Privacy Act of 1974, and the Future of RFID*, 2005 DUKE L. & TECH. REV. 20, at 1 (2005), *available at* http://www.law.duke.edu/journals/dltr/articles/pdf/2005dltr0020.pdf.

[21] *Id.*

RFID devices have been labeled "bar code[s] of the future," but they might, more accurately, be described as "bar code[s] on steroids."[22] The individualized microchips, each carrying unique information, can transmit the tag's location and a plethora of other personally identifiable information.[23] Unlike regular bar codes, RFID chips need not be in contact with a reader; in fact, a reader located even several feet away can communicate with the chip.[24]

In the last few years, reader sensitivity, range and processing speed have increased exponentially. While this increases efficiency, it also creates more threats to an individual's privacy. With sensitive readers that can receive signals quickly and through physical barriers, any hope of shielding personal information from wayward readers becomes quite difficult.

This increased sensitivity was demonstrated at the Fifth Annual RFID World Conference when Kevin Ashton, vice president of Think Magic, "stood on stage and easily read an RFID tag through a glass of water and another through a metal soup can–difficult feats just a year or two ago."[25] Ashton further discussed readers that can process "200 tags per second and work in close proximity to other readers without interference."[26] Furthermore, "the price of RFID [tags] has fallen as volumes have increased; before long, an RFID [tag] will sell for less than five cents."[27]

RFID critics often inflate their fears by "overlook[ing] or intentionally downplay[ing] the fact that extremely Orwellian RFID systems would require an integrated network of readers in addition to the ubiquitous affixation of tags."[28] Even once the price of an RFID reader falls, this technology is not likely to become the ultimate

[22] Smith, *supra* note 14, at 249 (quoting Denise Power, *On Track: With RFID a Hot Retail Topic, Footwear Companies are Developing Ways to Implement the New Technology–But They're Doing it Quietly*, FOOTWEAR NEWS, Oct. 31, 2006, at 14.).

[23] *E.g.*, Social Security numbers and credit card information. *See, e.g.*, Gilbert, *supra* note 2, at 3.

[24] Kevin Werbach, *Sensors and Sensibilities*, 28 CARDOZO L. REV. 2321, 2330 (2007).

[25] Corinne Kator, *RFID Industry Shifts Focus to Software*, MODERN MATERIALS HANDLING, April 3, 2007, http://www.mmh.com/article/CA6430374.html.

[26] *Id.*

[27] *Id.*

[28] Eden, *supra* note 20, at 11.

tracking system some privacy advocates fear.[29] However, since the technology is so simple, people are right to worry, for example, that identity thieves might use RFID readers to uncover important, private personal information, and with fears of RFID technology's proliferation, privacy advocates are rightly concerned about how information gathered will be regulated. The industry and the government must not take these concerns lightly.

III. RFID DEVICES HAVE BEEN EMPLOYED IN MANY FACETS OF LIFE

"RFID technology is not the stuff of science fiction novels. It is here today and . . . employed" in many facets of life.[30] Most RFID uses will have a positive effect on human health, efficiency, safety or security, but each use can lead to a potential invasion of privacy.[31] While many RFID uses offer society benefits that outweigh their associated privacy risks, some seem ripe for misuse.[32]

This section explores RFID uses that have either emerged or spread in the last few years, along with proposed future uses of RFID technology and the potential threat to privacy inherent in each. Both the federal government and private industry have integrated RFIDs into their daily operations in many ways. The uses are quite varied, ranging from making everyday tasks more efficient, protecting consumers from fraud, controlling supply chains and inventory,[33] making credit cards more secure, increasing national security and tracking humans and animals.[34]

[29] *See* RFID Journal, Frequently Asked Questions, The Cost of RFID Equipment, http://www.rfidjournal.com/faq/20 (last visited Jan. 20, 2008); *see also* Eden, *supra* note 20, at 11 ("Where video surveillance is . . . [limited], RFID tags could allow for accurate identification of individuals in a reader-rich environment.").

[30] Smith, *supra* note 14, at 250; *see* Gilbert, *supra* note 2, at 3.

[31] Eden, *supra* note 20, at 24.

[32] Smith, *supra* note 14, at 262; Gilbert, *supra* note 2, at 4.

[33] For a complete review of RFID use in inventory control, *see* Weinberg, *supra* note 1, at 777.

[34] *See* Eden, *supra* note 20, at 10.

A. MAKING LIFE EASIER FOR THE AVERAGE AMERICAN

RFID chips have become common throughout an ordinary American's life.[35] The following section examines four major uses of RFID technology: tollbooths, parking permits, baggage-tracking systems and consumer gadgets.

1. TOLLBOOTHS[36]

One of the oldest, most widespread and most visible uses of RFID is electronic toll collection.[37] When a vehicle with an RFID tag attached to its windshield passes through a tollbooth, a reader scans the tag and debits the driver's account.[38] Electronic toll collection eliminates long lines of traffic at tollbooths because drivers no longer have to "fish for quarters."[39]

Every time an RFID-labeled vehicle passes through a tollbooth, the reader records its presence; drivers sacrifice their privacy and anonymity for the convenience of not waiting in line.[40] These records have been used as important evidence in both civil[41] and criminal

[35] Americans already use RFID-tagged cards every day. Many student and employee identification and access cards have employed RFID technology for several years. They give the convenience of being able to swipe the card without even taking it out of a wallet. *See* PRIYA AGRAWAL ET AL., THE MIT ID CARD SYSTEM: ANALYSIS AND RECOMMENDATIONS (Dec. 10, 2004), http://www-swiss.ai.mit.edu/6095/student-papers/fall04-papers/mit_id/.

[36] *See* Burnham, *supra* note 2, 1507–20 (discussing privacy concerns that have arisen with the prevalence of electronic toll card); *see, e.g.*, Dan Ilett, *RFID Subway Pass? Sure, New York Says*, CNET NEWS.COM, Jan. 31, 2006, http://www.news.com/2100-1039_3-6033364.html (discussing how RFIDs are used for paying subway tolls in several American and European cities).

[37] *See, e.g.*, Wikipedia, EZ Pass, http://en.wikipedia.org/wiki/E-ZPass (last visited Jan. 20, 2008).

[38] Smith, *supra* note 14, at 257.

[39] Preserving Your Privacy and More, http://nestmannblog.sovereignsociety.com/2007/08/your-electronic.html (Aug. 14, 2007, 19:01 EST).

[40] Smith, *supra* note 14, at 257.

[41] WNBC.com, E-ZPass Now Hard on Adulterers in NJ, http://www.wnbc.com/news/13857158/detail.html?rss=ny&psp=news ("Of the 12 states in the Northeast and Midwest that are part of the E-ZPass system, agencies in seven states will provide electronic toll information in response to court orders for criminal and civil cases, including divorces, according to an Associated Press survey . . . . In another four states, including New Jersey and

cases.[42] Prosecutors and plaintiffs' attorneys regularly subpoena electronic toll records to determine "where an individual's car was at a particular time."[43] The records are also increasingly used to draw inferences about a driver's character, especially in divorce[44] and child custody[45] cases where the records can show travel time. The driver has reasonable expectation of privacy for tollbooth records, therefore the Fourth Amendment does not protect these records from being subpoenaed.[46]

As one prominent RFID critic has said, "people are foolish to buy into these systems without thinking [about the consequences of the RFID chip], just because they want to save 20 seconds of time going through a tollbooth."[47] This risk of tracking is entirely the driver's choice. If drivers do not want to be tracked when paying a toll, all they have to do is sacrifice the convenience of automatic toll payment, wait in line and pay in cash.

2. PARKING PERMITS[48]

The city of Hoboken, New Jersey, has embraced RFID technology as a means to combat its parking logistical nightmare.[49] Hoboken,

Pennsylvania, the use of E-ZPass records is limited to criminal cases. West Virginia doesn't have a policy.") (last visited Jan. 20, 2008).

[42] Smith, *supra* note 14, at 257.

[43] *Id.*

[44] Preserving Your Privacy and More, *supra* note 39 (quoting New York divorce lawyer Jacalyn Barnett) ("E-ZPass is an E-ZPass to divorce court, because it's an easy way to show you took the off-ramp to adultery.").

[45] Smith, *supra* note 14, at 257 (In an Illinois child custody case, "the husband's attorney subpoenaed the wife's I-Pass toll records to show that she often worked late, supporting an inference that she was not spending time with her children.").

[46] Preserving Your Privacy and More, *supra* note 39; *see* Burnham, *supra* note 2, at 1507–10 (citing United States v. Jackson, 207 F.3d 910, 914 (7th Cir. 2000), *vacated on other grounds*, 531 U.S. 953 (2000); United States. v. Forrest, 355 F.3d 942, 949 (6th Cir. 2004)); *see also* Reepal S. Dalal, Note, *Chipping Away the Constitution: The Increasing Use of RFID Chips Could Lead to an Erosion of Privacy Rights*, 86 B.U. L. REV. 485, 495–514 (2006).

[47] WNBC.com, *supra* note 41 (quoting Bob Barr, former Republican U.S. Representative turned Libertarian and privacy rights advocate).

[48] RFIDs have long been used for pre-paid parkers to gain entry into parking garages. *See, e.g.*, Delaney, *supra* note 1, at 557.

located just outside of New York City, is home to 40,000 residents who are "crammed into its one-square-mile borders."[50] The city also sees many commuters because it is located on a direct public transportation line between New Jersey and New York City.[51] With so many vehicles in a confined area, Hoboken was a huge traffic and parking disaster.[52] With only 4,000 outside parking spaces and 12,000 garage spaces, residents and commuters engaged in a daily battle for the few legal, available spaces.[53] Many clever parkers fooled authorities with out-of-date or fake parking permits, effectively stealing paying parkers' spaces.[54]

To stop these fraudulent parkers, in 2005, the city installed "RFID chips in all newly issued parking permits"; this gave parking enforcement officers the ability to distinguish between residents and non-residents, as well as to identify counterfeit permits, all in an instant.[55] In fact, any parking enforcement officer with an RFID-enabled laptop can now "get a read out on a host of information" including "the owner's name, address, registration number, phone number and permit specifications, as well as the location of the car and whether it's supposed to be where it is."[56] This enables legitimate parkers to find their assigned spaces without the hassle of fraudulent parkers stealing their spaces.

The city of Hoboken now has information on all of the cars (and associated drivers) parked within its borders, including "where they go [and] where they've been."[57] In fact, the city now knows exactly who its customers are, even down to their driving history.[58] Hoboken

[49] Renee Boucher Ferguson, *City of Hoboken Using RFID in Parking Permits*, EWEEK.COM, June 12, 2006, http://www.eweek.com/article2/0,1759,1975813,00.asp.

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] *Id.*

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] *Id.* (quoting John Corea, director of parking for the city of Hoboken).

[58] *Id.*

officials plan to use this information for many good reasons, including helping to understand parking behavior, and residents' travel habits.[59] "The city also plans to make the data available to police in investigations."[60]

The personal information is already known to the city when a resident applies for a parking permit, but the ability to track and record movements is new. Residents may not appreciate the city tracking their movements and parking habits. However, use of RFID-enabled parking permits has many advantages for both the city of Hoboken and its citizens. The city's parking ticket revenue has increased, and the data the city collects can help to "plot out future parking needs."[61] Residents can be sure that their assigned parking space will be available, eliminating the headaches of having to find another space. Residents, however, might be worried that they will lose their anonymity.

3. Baggage-tracking Systems

Mishandled "luggage may one day be a thing of the past."[62] RFID chips are poised to replace bar codes placed on baggage at airport check-ins, which will allow airlines to sort and route packages reliably, thereby reducing occurrences of late, lost or misdirected luggage.[63] RFID tags are so versatile that they even allow airports to update any revised information regarding flight changes and rerouting in real time, enabling the baggage to be sorted onto the correct flight.[64]

For consumers, RFID technology means "considerably less baggage hassle."[65] With today's bar code tags, 10% of bags are misread and subsequently mishandled.[66] RFID tags reduce the

[59] *Id.*

[60] *Id.*

[61] *Id.*

[62] Terry Gardner, *RFID: A Technology to Help Bring Your Luggage Home*, L.A. TIMES.COM, Oct. 10, 2007, http://travel.latimes.com/articles/la-tr-insider14oct14.

[63] *Id.*; *see also* Dalal, *supra* note 46, at 488.

[64] Dalal, *supra* note 46, at 488.

[65] Gardner, *supra* note 62.

[66] *Id.*

misreading rate to just 1%.[67] Currently, several airports have employed RFID technology, including Hong Kong International Airport and Las Vegas's McCarran International Airport, and other airports may soon follow their lead.[68] In fact, McCarran hopes to implement technology so sophisticated that it enables your bag to "text you and tell you where it is."[69]

RFID baggage tracking systems are a great advancement, ensuring luggage arrives at its destination and eliminating travelers' headaches. If the system is not well protected, however, the technological advancement could result in catastrophic consequences. For example, "a terrorist [may be able to debilitate] a baggage database in order to slip in a lethal suitcase" by infecting the entire network with a virus, effectively hiding baggage from security officials.[70] However, with proper protection, this RFID baggage claim could possibly be the most legitimate use of RFIDs and may be the least threatening to privacy.

4. CONSUMER GADGETS: NIKE + IPOD

In August 2006, Nike and Apple launched the Nike + iPod Sport Kit.[71] This technological advancement allows runners to "monitor distance traveled, calories burned and speed" via an RFID chip in their special Nike shoe and a reader in the iPod Nano.[72] Apple touts this device as an extremely convenient way for runners to keep track of

[67] Errors can occur if a tag slides under a bag handle. *Id.*

[68] San Francisco International Airport, Amersterdam's Schiphol Airport, Paris's Charles de Gaulle Airport and London's Heathrow International Airport are each in various stages of implementing RFID systems. *Id.*

[69] *Id.*

[70] Spychips.com, RFID 1984, RFID Vulnerable to Virus Attack Could Wreak Havoc, http://www.spychips.com/press-releases/rfid-virus.html (last visited Jan. 20, 2008).

[71] Smith, *supra* note 14, at 249–50; *see* Tom Espiner, *Nike + iPod Raises Privacy Concerns*, CNET NEWS.COM, Dec. 13, 2006, http://www.news.com/2100-1029_3-6143606.html; *see also* Apple, Nike + iPod, http://www.apple.com/ipod/nike/ (last visited Jan. 20, 2008).

[72] Smith, *supra* note 14, at 250.

their workouts in real-time.[73] But Nike + iPod Sport Kit users may be unwittingly putting themselves at risk of surveillance.[74]

Researchers at the University of Washington's computer science department have discovered that the Nike + iPod device is not only an exercise tool, but also a surveillance device.[75] The scientists revealed several problems inherent in the Nike + iPod device. First, "the RFID in the shoe sensor contains its own on-board power source, essentially turning your running shoe into a small radio station capable of being received from up to 60 feet away with a signal powerful enough to be picked up from a passing car."[76] Second, the sensor reveals its unique ID to "any Nike + iPod receiver."[77] Researchers found that the hardware is so easy to hack that "any high school student could do it in the garage."[78] For example, a scorned lover could hack into his girlfriend's Nike + iPod system and discover exactly where she is running and at what times.

Beyond simple hackers, this technology might be attractive to the corporate world. In fact, it would be quite easy, and possibly quite lucrative, "for a company to build their own tiny readers and deploy them in a large environment, selling the data stream to those who would track spouses or teens, or collect information about how many people wearing Nikes visit malls or movie theaters."[79] Retailers are not likely to employ this technology, however, because they have little motivation to invade customers' privacy.[80] The public backlash would probably be reason enough to dissuade retailers from employing such technology.

[73] *See* Apple, Nike + Apple–Rock 'n Run, http://www.apple.com/ipod/nike/run.html (last visited Jan. 20, 2008) ("With a sensor in your shoe and a receiver on your iPod nano, your run takes on a whole new dimension.").

[74] Annalee Newitz, *Nike + iPod = Surveillance*, WIRED, Nov. 30, 2006, http://www.wired.com/science/discoveries/news/2006/11/72202.

[75] *See* T. Scott Saponas et al., *Devices that Tell on You: The Nike + iPod Sport Kit*, Nov. 30, 2006, http://www.cs.washington.edu/research/systems/nikeipod/tracker-paper.pdf.

[76] Newitz, *supra* note 76.

[77] *Id.*

[78] *Id.* (quoting University of Washington computer science professor Yoshi Kohno).

[79] *Id.*

[80] Laura Hildner, Note, *Defusing the Threat of RFID: Protecting Customer Privacy through Technology-Specific Legislation at the State Level*, 41 HARV. C.R.-C.L. L. REV. 133, 142 (2006), *available at* http://www.law.harvard.edu/students/orgs/crcl/vol41_1/hildner.pdf.

A spokesman for the Electronic Frontier Foundation has noted, "this isn't just a problem with the Nike + iPod per se–it's a cautionary tale about what happens when companies unwittingly build a surveillance capacity into their products."[81] This easily engineered surveillance capability "shows a need for independent oversight and investigation of these technologies before they go to market."[82] Companies potentially put consumers at risk when they release products like the Nike + iPod Sport Kit without adequately considering the potential associated privacy abuses.[83]

B. PROTECTING AMERICAN CONSUMERS FROM COUNTERFEIT PHARMACEUTICALS

Counterfeit drugs put patients' lives at risk.[84] No American should ever worry that the drug she is taking is not exactly what the doctor ordered.[85] Unfortunately, this threat is real because the American pharmaceutical supply chain is highly vulnerable.[86] Recognizing this reality, Congress passed the Prescription Drug Marketing Act of 1987 ("PDMA")[87] to ensure consumers receive authentic products and to make it significantly more difficult for counterfeiters to introduce their

[81] Newitz, *supra* note 76 (quoting Lee Tein, staff attorney for the Electronic Frontier Foundation).

[82] *Id.* (quoting David Molnar, RFID researcher at the University of California, Berkeley).

[83] *Id.*

[84] For a review of international drug counterfeiting and the American legal response, *see* Tim Gilbert & Sana Halwani, *Confusion and Contradiction: Untangling Drug Importation and Counterfeit Drugs*, 36 CAL. W. INT'L L. J. 41 (2005–06); *see also* Donald deKeiffer, *Trojan Drugs: Counterfeit and Mislabeled Pharmaceuticals in the Legitimate Market*, 32 AM. J. L. & MED. 325 (2006).

[85] Robert P. Giacalone, *Drug Wholesaling and Importation: Challenges and Opportunities*, 36 CAL. W. INT'L L.J. 65 (2005–06).

[86] Paul Faber, *RFID Strategy–Pharmaceutical E-Pedigrees and RFID*, INFOWEEK: INDUSTRYWEEK, Oct. 16, 2007, http://www.industryweek.com/ReadArticle.aspx?ArticleID=15180&SectionID=2 ("Pharmaceuticals pass through many different points in the distribution chain from the factory to your local pharmacist. This leaves the system vulnerable to the introduction of counterfeit drugs.").

[87] Prescription Drug Marketing Act of 1987, Pub. L. No. 100-293, 102 Stat. 95 (1988); Prescription Drug Amendments of 1992, Pub. L. No. 102-353, 106 Stat. 941 (1992).

products into the supply chain.[88] The Food and Drug Administration ("FDA") believes "that RFID is the most promising technology to meet [the goals of the PDMA]," making the task of tracking the chain of custody more secure and less labor intensive.[89] Thus, since 2004, the FDA has investigated how to use RFIDs for this purpose.[90] In fact, the FDA believes that the "use of RFID technology is critical to ensuring the long-term safety and integrity of the U.S. drug supply."[91] However, mass implementation has been met with considerable resistance and has yet to be implemented on a national scale.[92]

Even with the FDA's recommendation, pharmaceutical companies have been hesitant to implement RFID tracking technology. Companies are dissuaded by the up-front costs of RFID implementation and the lack of an immediate return on their investment.[93] They are also concerned that "if RFID tags containing identifying information were still on the drugs when they were sold, [the drug companies] could be found liable if unauthorized individuals were to intercept personal information without the purchasers' knowledge."[94] Since RFID tags and associated company databases have the potential to carry a large amount of personal information, companies fear that the information might be all too easily accessible to hackers.[95] Also, until recently, each RFID vendor set its own

[88] RFID Product News, IBM's FDA Advisor Speaks Out about the FDA's New Anti-Counterfeiting Measures, http://www.rfidproductnews.com/issues/2006.07/speakout.php (last visited Jan. 20, 2008).

[89] FDA COUNTERFEIT DRUG TASK FORCE REPORT: 2006 UPDATE (JUNE 2006), http://www.fda.gov/oc/initiatives/counterfeit/report6_06.html; *see* Faber, *supra* note 86; *see also* Giacalone, *supra* note 85, at 65.

[90] Faber, *supra* note 86.

[91] FDA, COMPLIANCE POLICY GUIDE 160.900, PRESCRIPTION DRUG MARKETING ACT–PEDIGREE REQUIREMENTS UNDER 21 CFR PART 203, Nov. 2006, http://interactive.snm.org/docs/fda_pdma-cpg_160-900_11-15-2006.pdf.

[92] Ronald Quirk, *E-Pedigree's Evolution,* RFID J., Mar. 5, 2007, http://www.rfidjournal.com/article/articleprint/3109/-1/1 ("[F]ewer than 10 types of prescription drugs are currently being tagged upon entering the supply chain."); *see* Beth Bacheldor, *U.S. Judge Issues Injunction Against Drug-Pedigree Rules*, RFID J., Dec. 8, 2006, http://www.rfidjournal.com/article/articleview/2882/1/1/.

[93] *Id.*

[94] *Id.*

standards, leading to incompatible equipment and "high overall costs and inefficiencies."[96]

Several states[97] have enacted laws to stop counterfeiting; each has different compliance requirements, yet none requires RFID chips.[98] However, Congress could soon implement a federal RFID requirement because many of its members support aggressively protecting Americans from counterfeit drugs.[99]

Several large drug companies have begun to implement RFID devices because of a recent change in RFID industry standards, as well as the fact that the money lost through counterfeit drugs far outweighs the cost of implementing RFID technology.[100] RFID technology also allows "trading partners to share data, improve inventory control, facilitate recalls and withdraw products with expired use dates."[101] Privacy advocates fear that patient privacy might have the potential to be compromised because pharmaceutical makers often put the RFID tag under the label "without any ability for the retail pharmacy to kill or destroy the tag," and regulations are not entirely clear as to what patient identifying information will be contained on the tags.[102] The only way to eliminate these fears is by educating consumers and developing regulations governing the kinds of information that may be contained in or linked to each RFID chip.[103]

[95] *Id.* Personal data contained on RFID chips could include names, addresses and phone numbers, as well as personal medical information.

[96] *Id.*

[97] *Id.* (*e.g.*, California, Florida, Nevada and Virginia).

[98] *Id.* ("Many drug companies are now avoiding the upfront costs of RFID by using less expensive alternatives, such as bar codes and paper, to comply with these laws.").

[99] *Id.* The U.S. House of Representatives has a bill in committee entitled, The Reducing Fraudulent and Imitation Drugs Act of 2007, H.R. 2716, which would require all prescription drugs to be tagged with RFID or similar technology to create an e-pedigree for tracking purposes. *See* Reducing Fraudulent and Imitation Drugs Act of 2007, H.R. 2716, 110th Cong., *available at* http://www.govtrack.us/congress/bill.xpd?bill=h110-2716.

[100] Quirk, *supra* note 92.

[101] *Id.*

[102] Letter from Matthew J. Leonard, Senior Vice President, CVS/Pharmacy, to the FDA (Feb. 24, 2006), http://www.fda.gov/ohrms/dockets/dockets/05n0510/05N-0510-EC22-Attach-1.pdf.

[103] *See* DANIEL W. ENGELS, EXECUTIVE SUMMARY, ON DRUG PEDIGREE AND RFID IN THE PHARMACEUTICAL SUPPLY CHAINS: A RECOMMENDATION TO THE FDA, at 1 (Feb. 24, 2006), http://www.fda.gov/ohrms/DOCKETS/dockets/05n0510/05N-0510-EC26-Attach-1.pdf.

Even with the potential privacy risk, the benefits to consumers of eliminating dangerous counterfeit drugs from the supply chain are indisputable.[104]

C. CONTACTLESS ACCESS TO CREDIT CARDS AND PERSONAL MEDICAL INFORMATION[105]

RFID tags may revolutionize the way consumers conduct credit card transactions by eliminating the need for swiping and signing; in fact, a credit card may never have to leave a wallet again.[106] Retailers that have "big cash business[es] and young audience[s]" feel that accepting contactless credit cards is the right move because "it's a form of payment everyone is going to want to use," allowing faster lines in which buyers spend more money, subsequently increasing the business's revenue.[107]

These contactless credit cards are possibly the RFID use that is most ripe for abuse.[108] "Major credit card companies, including Visa, MasterCard, and American Express have issued tens of millions of

[104] One potential future use of RFIDs in the pharmaceutical industry is a far greater threat to patient privacy. Accenture "has patented a design that builds an RFID reader into a household medicine cabinet," ensuring that a patient takes all his medications and that none of the medications have negative interactions. While this invention is quite helpful for the elderly patient with many prescriptions, it also raises fears that one day drug companies, or even the government, might track the contents of a person's medicine cabinet. Hiawatha Bray, *You Need Not be Paranoid to Fear RFIDs*, BOSTON GLOBE, Oct. 10, 2005, http://www.boston.com/business/globe/articles/2005/10/10/you_need_not_be_paranoid_to_fear_rfid/?page=2.

[105] For a complete analysis, *see* Weinberg, *supra* note 1.

[106] RFIDs are also being considered for use in currency. *See* Electronic Privacy Information Center, RFID Systems, http://www.epic.org/privacy/rfid/ (last visited Jan. 20, 2008); *see also* Prison Planet, RFID Tags in New US Notes Explode When You Try to Microwave Them, http://www.prisonplanet.com/022904rfidtagsexplode.html (last visited Jan. 20, 2008); *contra* Spychips.com, RFID 1984, FAQ, http://www.spychips.com/faqs.html (last visited Jan. 20, 2008) ("To the best of our knowledge, US currency does NOT currently contain RFID chips.").

[107] *Smart Card Alliance Conference Day 2 Roundup*, SECUREID NEWS, Oct. 13, 2007, http://www.secureidnews.com/news/2007/10/13/smart-card-alliance-conference-day-2-roundup/ (quoting Kevin Rochlitz, senior director for the Baltimore Ravens) [hereinafter *Smart Card Alliance Conference*].

[108] Smith, *supra* note 14, at 259.

cards using RFID."[109] There are as many as 150,000 contactless payment terminals to read these contactless credit cards in 55,000 retail locations in the United States, with many more to come.[110] However, this usage is significantly less than what was forecasted in 2004 by Jupiter Research, which predicted by 2009, 396 million contactless credit cards would be in use, resulting in 2.9% of all purchases.[111] Several major U.S. cities and credit card companies are exploring the advantages of using contactless credit cards on city buses and subways because "it's the fastest way to get on a bus or enter the subway."[112]

Even though industry experts have touted contactless payment as "fun, cool, safe, and easy–at a manageable expense" and credit card companies use "128-bit encryption and other security features to protect their contactless devices," fears about the security of these credit cards have tempered user enthusiasm.[113] This fear seems to be justified. Researchers have demonstrated that these credit cards can be read through "wallets, clothing, and envelopes."[114] Even though the distance at which a card could be read is rather short, a thief even a few feet away could pull credit card data from wallets of people in a crowd or even from an envelope sitting in a mailbox.[115] While "credit card companies have marketed the cards as secure by means of encryption," two University of Massachusetts Amherst computer scientists, Tom Heydt-Benjamin and Kevin Fu, were able to make an

[109] *Id.*

[110] *Smart Cards Key to Mobility and Security from Payment to Personal Healthcare Records*, MORERFID, Oct. 18, 2007, http://www.morerfid.com/details.php?subdetail=Report&action=details&report_id=3681&display=RFID ("BP will start accepting [Master Card's] PayPass at 3,000 U.S. locations next year[;] Coca Cola is installing contactless [readers] at 7,500 additional vending machines and more than a dozen airports have committed to accepting contactless payment including Atlanta, Chicago, Philadelphia and Dallas.").

[111] Steve Mott, *Why Once-Soaring Contactless Payment Has Lost Some Altitude*, DIGITAL TRANSACTIONS, Sept. 27, 2007, http://www.digitaltransactions.net/newsstory.cfm?newsid=1528.

[112] *Smart Card Alliance Conference*, *supra* note 107 (quoting Jonathan Davis, deputy general manager and CFO of the Massachusetts Bay Transportation Authority).

[113] *Id.*

[114] Smith, *supra* note 14, at 259.

[115] *Id.*

RFID reader out of common computer and radio components and read RFID chips in credit cards.[116] Not only did they find the cardholder's name in plain text, but they also found the credit card number and expiration date.[117] They tested "20 cards actually issued by three payment brands, and each and every one was exposed."[118]

Proponents argue that contactless credit cards are safer than traditional cards because one at least needs to have a reader to steal the account information, as opposed to an ordinary card, which has the consumer's name, account number, card expiration date, and Card Verification Number in plain visual display, so anyone who could see the card could steal all of the relevant information.[119] However, with contactless credit cards, a thief does not even need to see the card. Consumers with an easily breached credit card who are subject to identity theft "could have a cause of action based on unfair trade practice and state data breach."[120] Researchers have already demonstrated the vulnerability of RFID-enabled contactless credit cards.[121] So "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."[122]

Even with these vulnerabilities, contactless card technology is extremely attractive to the healthcare industry,[123] which sees a benefit

[116] *Id.*; *see* John Schwartz, *Researchers See Privacy Pitfalls in No-Swipe Credit Cards*, N.Y. TIMES, Oct. 23, 2006, http://www.nytimes.com/2006/10/23/business/23card.html?_r=1&oref=slogin.

[117] Schwarz, *supra* note 116.

[118] Mott, *supra* note 111.

[119] *Id.*

[120] Smith, *supra* note 14, at 270. Additionally, the Fair Credit Billing Act limits unauthorized charges to $50, were the card to be used by thieves. *See* Federal Trade Comm'n, Credit, ATM or Debit Cards: What to do if They're Lost or Stolen, http://www.ftc.gov/bcp/conline/pubs/credit/atmcard.shtm (last visited Jan. 20, 2008).

[121] Smith, *supra* note 14 at 270.

[122] *Id.*

[123] *See* Laurianne Mclaughlin, *Hospital Puts Medical Records Snapshot on Smart Cards*, NETWORKWORLD, Oct. 18, 2007, http://www.networkworld.com/news/2007/101807-hospital-puts-medical-records-snapshot.html; *see also Smart Card Alliance Conference*, *supra* note 107 (Mount Sinai hospital in New York has started a pilot program using these contactless,

in using these cards as "a personal, portable patient record" with the power to "speed[] up registration, reduc[e] fraud, improv[e] the quality of care and provid[e] rapid access to critical information in an emergency."[124] These personal patient records contain secure, encrypted patient identification and insurance information, current prescriptions, allergies and recent medical history, which should help avoid medical errors and duplicate procedures.[125] These personal records even could contain an EKG or other medical tests, "something emergency room doctors say can be extremely valuable in an emergency, but is hard to come up with when every second counts."[126]

In this setting, patients must first enter a personal identification number before healthcare professionals can access any of the information on the chip.[127] These personal medical records provide a real advantage over the obsolete paper charting systems. Given the ease of hacking into "secure" credit cards, however, it might be hard to trust the privacy and security of these personal medical cards. The government, with cooperation from the medical community, must set and enforce strict standards for patient privacy.

D. NATIONAL SECURITY[128]

Following the terrorist attacks of September 11, 2001, the government has become increasingly interested in RFID technology. The government believes that RFID tags will act as a means to increase national security, protect nuclear materials, and secure our nation's borders[129] and ports.[130]

portable patient records with other New York hospitals and hospitals around the country soon following.).

[124] *Smart Card Alliance Conference*, *supra* note 107.

[125] *Id.*

[126] *Id.*

[127] *Id.*

[128] For a review of U.S. e-passports, *see* Francis Fungsang, Note, *Information Collection: U.S. E-Passports: ETA August 2006: Recent Changes Provide Additional Protection for Biometric Information Contained in U.S. E-Passports*, 2 ISJLP 512 (2006).

[129] *See* ELEC. PRIVACY INFO. CTR., NOTICE OF PROPOSED RULEMAKING: MINIMUM STANDARDS FOR DRIVER'S LICENSES AND IDENTIFICATION CARDS ACCEPTABLE BY FEDERAL AGENCIES FOR OFFICIAL PURPOSES (2007), http://www.epic.org/privacy/id_cards/epic_realid_comments.pdf ("[T]he Department of Homeland Security ("DHS") has just abandoned a plan to include RFID chips in border identification documents because the pilot test was a failure.").

Since January 1, 2007, all U.S. passports have included an active RFID tag, containing the person's name, nationality, date of birth and digitized photograph.[131] The goal of these technologically advanced passports is to "make forgeries of passports more difficult" in an attempt to enhance national, and international security.[132]

Another troubling aspect of the government trying to control national security through RFID was born from the REAL ID Act of 2005.[133] "REAL ID is a nationwide effort," recommended by the 9/11 Commission, "intended to prevent terrorism, reduce fraud, and improve the reliability and accuracy of identification documents that State governments issue."[134] The REAL ID Act requires anyone traveling "domestically by airplane to have a state-issued ID that complies with the Act's standards."[135] In an effort to "thwart counterfeits and forgeries," as well as to increase the efficiency of identification and verification, the federal government may mandate all states to issue drivers licenses with embedded RFID tags.[136] States, however, have bitterly opposed a driver license requirement as an underfunded mandate. As a result, on March 1, 2007, the Department of Homeland Security decided not to require states to implement RFID technology in REAL IDs.[137]

The thought of having so much personally identifiable information on an RFID chip is alarming because chips similar to the ones used on U.S. passports have been compromised by hackers quite easily. "In February 2006, the prototype for the RFID Dutch e-passport was

[130] For an introduction of how RFIDs will be employed at ports, *see* Mark Schrope, *Screening System Protects Ports from Deadly Cargo*, CNN.COM, June. 30, 2007, http://www.cnn.com/2007/TECH/06/27/sentinels.at.sea/index.html?iref=newssearch.

[131] Smith, *supra* note 14, at 260; *see* Fungsang, *supra* note 128.

[132] Dalal, *supra* note 46, at 490.

[133] REAL ID Act of 2005, Pub. L. No. 109-13, Div. B, 119 Stat. 231 (2005).

[134] Dep't of Homeland Sec., REAL ID Proposed Guidelines: Questions and Answers, http://www.dhs.gov/xprevprot/laws/gc_1172767635686.shtm (last visited Jan. 20, 2008).

[135] Smith, *supra* note 14, at 260; *see* Gina M. Scott, *Real ID Act Deadline Pushed Back to 2009*, GOVERNMENT TECHNOLOGY, Mar. 1, 2007, http://www.govtech.com/gt/104173 ("[S]tates will now have until December 31, 2009 to implement the regulations of the Real ID act.").

[136] Dalal, *supra* note 46, at 490.

[137] Dep't of Homeland Sec., *supra* note 134.

cracked on national television," where "in less than two hours," hackers were able to crack the encryption, allowing "full access to all the information on the passport."[138] "In November 2006, the technology protection on three million British e-passports was cracked by software written in less than 48 hours and an RFID reader bought for about $500."[139] Also in 2006, just a month after the U.S. began issuing RFIDs in passports, hackers released a code on the Internet that allowed people to hack into the chips.[140]

Similarly, in August 2006, "security researcher Jonathan Westhues showed the vulnerability of high security areas that rely on RFID-embedded card entry systems" by hacking into the "RFID-embedded entry cards of two California state legislators."[141] By hacking these entry cards, Westhues was able to transmit the information from his laptop and gain access to the secure California State Capitol building as an assembly member.[142]

RFID-chipped passports, driver licenses and access cards help to ensure national security, but also give the government "limitless surveillance potential"; these chips contain "highly sensitive personal information about citizens' whereabouts and identity."[143] Identity thieves and other criminals would love to get their hands on such personal information and they might be able to because the information is transmitted through easily intercepted radio waves.[144] Potentially even more frightening is the fact that the government "will be able to lawfully access personal information from citizens' passports and driver licenses without citizens' knowledge or consent . . . from more than 50 feet away."[145] Eventually, the government might be able to link RFID devices in passports or driver licenses with GPS systems, which would enable the government to "form a

[138] Ozer, *supra* note 10, at 11.

[139] *Id.* at 8.

[140] Posting of Christopher Null to Yahoo! Tech, http://tech.yahoo.com/blog/null/6808 (Oct. 31, 2006, 3:36 EST).

[141] Ozer, *supra* note 10, at 10.

[142] *Id.*

[143] Dalal, *supra* note 47, at 493.

[144] *Id.*

[145] *Id.*

comprehensive picture of the comings and goings of its citizens."[146] While these threats are not likely to impact the average American, policymakers should consider these possible consequences.

E. TRACKING PEOPLE

RFID tags are also used to track people. Every use has a positive intention. For example, some schools,[147] and even an amusement park,[148] have employed RFID devices to track children so they do not get lost or kidnapped.[149] Some nursing homes use similar technologies to prevent Alzheimer's patients from wandering off the premises.[150] RFID chips are also used in proximity cards to allow authorized people to gain access to "buildings or other protected areas."[151]

While proximity cards, for the most part, keep unauthorized people out of buildings, they also provide an efficient tracking mechanism to monitor the entrances and exits from a specific area.[152] They also allow employers or others to track people through buildings and even record how long they stay in one place, possibly inferring that they are socializing instead of working.[153] While this may make for a more efficient work place, it could also be a breach of privacy. Thus, employers must weigh the legitimate need for the information against the cost of spying on employees' lives and habits.[154] While, in some circumstances, it may be necessary for employers to have information about employees, the devil is in the details regarding how to get the information and use it in the least privacy-invasive way.

[146] *Id.*

[147] *See* Smith, *supra* note 14, at 260; *see also* Ozer, *supra* note 10, at 1.

[148] *See* Kelly Shermach, *Legoland RFID Tracks Lost Kids, Collects Data*, CRM BUYER, Oct. 28, 2004, http://www.crmbuyer.com/story/Legoland-RFID-Tracks-Lost-Kids-Collects-Data-37694.html.

[149] Gilbert, *supra* note 2, at 3.

[150] *Id.* at 4.

[151] *Id.*

[152] *Id.* at 10.

[153] *Id.*

[154] *Id.*

Proximity cards and other similar tracking technologies are all "worn outside the body and thus [can] be removed," giving the person wearing the RFID the choice not to carry or wear the RFID tag.[155] With subdermal chips, the person loses that choice. Subdermal chips are now a reality, since the FDA approved the VeriChip™, an implantable RFID chip.[156] Hospitals and healthcare providers, as well as employers, see the potential benefits of implanting humans with a microchip, from instant medical histories and personal health records to tracking an employee through his day, both turning on efficiency.[157]

One major problem with this implant is that it might not be medically safe.[158] A series of veterinary studies from the 1990s showed a link between malignant tumors in animals and microchips.[159] There is a question whether this animal model can be applied to humans, but perhaps the FDA was premature to approve the VeriChip™ until its link to cancer could be fully characterized and understood.

Privacy advocates argue that the potential for unauthorized access to medical records is still too high a risk for any hospital to take with its patients' records.[160] Similarly, they argue that employers mandating employees to get chipped could be overstepping the bounds of their employment relationship.[161] Under both circumstances, the likelihood of "invasive data aggregation, improper violations of anonymity and other violations of personal privacy" is higher than in many of the other RFID uses described above.[162] "The ramifications

[155] Smith, *supra* note 14, at 260.

[156] Eden, *supra* note 20, at 10–11.

[157] *See id.* (discussing why hospitals are excited about the Verichip™); *see also* Smith, *supra* note 14, at 265 (discussing why employers are excited about the VeriChip™); *see also* Company Requires RFID Injection, Feb. 10, 2006, http://www.securityfocus.com/brief/134 (last visited Jan. 20, 2008) (describing an example of an employer who is interested in microchipping its employees).

[158] Eden, *supra* note 20, at 10–11.

[159] Todd Lewan, *Chip Implants Linked to Animal Tumors*, WASH. POST, Sept. 8, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/08/AR2007090800997_pf.html.

[160] Eden, *supra* note 20, at 10–11.

[161] Smith, *supra* note 14, at 261–62.

[162] Eden, *supra* note 20, at 10-11.

of RFID implants imply that people could be tracked anywhere, anytime–in both public and private places."[163] The fact that these chips can be implanted, without the ability to remove them easily, might give them a negative connotation.[164]

Several states have recently adopted laws prohibiting the non-consensual implantation of microchips into human subjects.[165] These regulations are just in time. In 2006, Westhues cracked the VeriChip™ in "less than two hours."[166] Then, after the chip is cloned and read, "the copy could be used for whatever purpose was intended for the initial chip," from reading a patient's confidential medical information to accessing a secured location.[167] These implantable chips hold perhaps the greatest potential for abuse, because they might contain links to the most intimate personal information: medical, biological, identifiable and locational. Thus, this technology requires the strictest government response. At the simplest level, these statutes should mandate notice and individual control. Ideally, these statutes should prevent employers from tracking their employees or invading their privacy.

IV. CONCLUSION

With RFID technology, "[t]he cost of the sacrifice of privacy is hard to quantify while the touted benefits seem hard for many people to overvalue."[168] Maybe the government and private industry are right to tout the exceptional benefits to efficiency, privacy and security.

[163] Smith, *supra* note 14, at 265.

[164] Many applications are positive, especially when they follow the FDA's guidelines; *see* Patricia Kaeding, *RFID Medical Devices–Opportunities and Challenges*, WISCONSON TECH. NETWORK, Oct. 19, 2005, http://wistechnology.com/article.php?id=2384.

[165] *See* Orr Shtuhl, *Lawmakers Fight Implanting of Microchip Tags in Humans*, DETROIT FREE PRESS, Sept. 25, 2007, http://www.freep.com/apps/pbcs.dll/article?AID=/20070925/NEWS07/709250367/1009; *see also* Anita Ramasastry, *Outlawing Employer Requirements that Workers Get RFID Chip Implants: Why it's the Right Thing to Do, Although Current Statutes May Need Refinement*, FINDLAW, Oct. 16, 2007, http://writ.news.findlaw.com/ramasastry/20071016.html.

[166] Ozer, *supra* note 10, at 11–12.

[167] *Id.* at 12.

[168] Kathleen Wallman, *The Tension Between Privacy and Security: An Analysis Based on Coase and Pigou*, 3 J. TELECOMM. & HIGH TECH. L. 397, 401 (2004–05).

Perhaps the threat to personal privacy is not as great as some privacy advocates fear. The most significant limitation to RFIDs' tracking capabilities is that the power level of the chip must be quite low so as not to interfere with other devices using radio frequency.

One real privacy threat comes not from RFID devices themselves, but from hackers. In fact, hacking seems to be getting easier by the day. Plus, mobile phone vendors are looking into developing portable RFID readers coupled with cellular phones, making "RFID technology a user-driven activity in addition to one controlled by companies."[169] If any teenage hacker with a cell phone can access personal information held on an RFID, it makes for quite an alarming proposition.

[169] Werbach, *supra* note 24, at 2331–32.