RIDING THE WAVE:

THE UNCERTAIN FUTURE OF RFID LEGISLATION

*Kyle Sommer**

I. INTRODUCTION

A global technological revolution is underway.[1] Most of us are oblivious to it, but we nevertheless directly contribute to its cause as we carry out our everyday lives. Remember your morning commute when you swiftly passed through the traffic toll booth without having to stop or scurried to make the next subway train after casually tapping your mass transit card at the turnstile? Or your lunch break, when you quickly purchased a sandwich with your smart card credit card without having to remove the card from your wallet? Or that time you walked out of a retail store, only to be stopped by the embarrassing sound of the alarmed sensors because the security tag on your new CD was not deactivated at the counter? If you are familiar with any of these scenarios then you have already been introduced to the "micro monitoring"[2] world of radio frequency identification, better known as RFID.

Like other new technologies, RFID is subtly, yet pervasively seeping into the framework of society. From cell phones, to email, to HD quality plasma TVs, we were not entirely conscious of their introduction though our dependence on these innovations quickly became steadfast, leaving us to wonder how we ever survived without them. To that list of technologies we now add RFID.

Industry has successfully maintained a relatively low profile with the rollout of RFID.[3] In a study of 8,500 adults conducted in April 2005, only 41

---

* Kyle Sommer, J.D., Notre Dame Law School, 2009. The author has a B.A. in Political Science and a B.A. in Spanish from the University of Washington. Thanks to Julie Mayer, attorney at the Federal Trade Commission, for introducing me to RFID and for her suggestions on this article, and to my parents for their unconditional love, steadfast support, and unbridled encouragement.

1. Rapid development of RFID technology has been deemed the "quiet revolution," giving rise to "pervasive commerce." Pervasive commerce describes the use of technologies such as tracking devices and smart labels embedded with transmitting sensors and intelligent readers to convey information about key areas where consumers live and work to data processing systems. *See* Electronic Privacy Information Center, Radio Frequency Identification (RFID) Systems, http://epic.org/privacy/rfid (last visited Apr. 1, 2009) [hereinafter EPIC].

2. Senator Patrick Leahy, The Dawn of Micro Monitoring: Its Promise and Its Challenges to Privacy and Security, Remarks at Georgetown University Law Center Conference on Video Surveillance: Legal and Technological Challenges (Mar. 23, 2004), *available at* http://leahy.senate.gov/press/200403/032304.html.

3. KATHERINE ALBRECHT & LIZ MCINTYRE, SPYCHIPS: HOW MAJOR CORPORATIONS AND GOVERNMENT PLAN TO TRACK YOUR EVERY PURCHASE AND WATCH YOUR EVERY MOVE, 37-53 (2005) (highlighting industry solutions of "hiding" the RFID tag—such as embedding it in clothing labels, the soles of shoes, and even in between layers of cardboard).

percent of those questioned had even heard of RFID.[4] This was an improvement from a survey six months earlier, where only 28 percent had heard of the technology.[5] This upward trend of public awareness is likely to continue with experts predicting explosive growth in the RFID market over the next decade.[6]

To the surprise of many, RFID boasts a plethora of uses already on the market.[7] While RFID has many benefits, privacy advocates have raised concerns that business and government will link individuals' identities to uniquely numbered items and thereby track peoples' movements. Lawmakers around the country have responded by scrambling to introduce legislation that would constrain the new technology. To the distain of RFID opponents, most RFID restricting legislation has not been widely accepted, leaving open the question as to what lies ahead for RFID.

This Note chronicles the use of RFID technology in the United States, the privacy concerns associated with its use, and the future of RFID legislation in light of changing public views regarding data privacy. Part I describes RFID and its technological underpinnings; limitations and benefits; and current and future applications. Part II considers the privacy concerns inherent in RFID technology as well as various viewpoints on the best way to address them. Part III explores RFID legislation at both the federal and state levels. Finally, Part IV discusses the future of RFID legislation in light of the public's attitude toward RFID and privacy issues generally.

II. WHAT IS RFID?

A. *RFID: The "Next Generation Bar Code"*[8]

Radio Frequency Identification (RFID) is a type automatic identification

---

4. Jonathan Collins, *Consumers More RFID-Aware, Still Wary*, RFID JOURNAL, Apr. 8, 2005, www.rfidjournal.com/article/articleview/1491/1/1/.

5. *Id.*

6. Reik Read of Baird expects RFID market to swell from $2.8 billion in 2006 to $8.1 billion by 2010. *See Radio Silence*, THE ECONOMIST, June 7, 2007, http://www.economist.com/printedition/displaystory.cfm?story_id=9249278 (last visited April 1, 2009); *see also* DAVID C. WYLD, RFID: THE RIGHT FREQUENCY FOR GOVERNMENT 8 (2005), http://www.businessofgovernment.org/pdfs/WyldReport4.pdf (projecting the RFID market to be worth $25 billion by 2015; *But see, Radio Silence*, THE ECONOMIST, June 7, 2007, http://www.economist.com/printedition/displaystory.cfm?story_id=9249278 (questioning how far RFID will go).

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

8. *Maxwell Introduces New RFID Solutions*, RFID GAZETTE, Mar. 29, 2005, http://www.rfidgazette.org/2005/03/maxell_introduc.html.

system ("Auto-ID").[9] Auto-ID[10] is a broad term assigned to technologies that are designed to help machines identify objects and include barcodes, smart cards, voice recognition, biometric technologies (e.g., retinal scans), optical character recognition (OCR) and now, RFID.[11] Unlike other Auto-IDs such as bar codes, RFID is a relatively small[12], fast, [13] technology "that enables tracking and monitoring activities to be carried out using invisible radio waves over distances that range from less than a centimet[er] to many hundreds of met[er]s."[14] From these imperceptible characteristics of RFID originate a variety of privacy concerns.

Radio Frequency Identification (RFID) describes a system that uses electronic waves to identify an object or person.[15] This system involves three key components: (1) tag, (2) reader, and (3) database.[16] The RFID tag consists of radio antenna attached to a microchip.[17] These microchips have the capacity to store a variety of information, including item-specific Electronic Product Code (EPC) identifiers, information about the item itself including consumption status or product freshness, or personal identification such as a bank account or social security number.[18] Although much of the debate for RFID has centered around the RFID tags, RFID readers and databases play an integral role because the data contained on a tag cannot be read without an appropriate reader. The RFID reader, which can either be a portable or fixed at strategic points, such as dock doors or an assembly line, is a device equipped with one or more antennas that emits radio waves, receive signals back from proximate RFID tags,

---

9. KLAUS FINKENZELLER, RFID HANDBOOK: FUNDAMENTALS AND APPLICATIONS IN CONTACTLESS SMART CARDS AND IDENTIFICATION 2 (Rachel Waddington trans., 2d ed. 2003).

10. The Auto-ID Center was set up in 1999 to develop a system for using the internet to identify goods anywhere in the world using the Electronic Product Code (EPC). Originally based at the Massachusetts Institute of Technology in Cambridge, MA the Auto-ID Center was supported by the Uniform Code Council and EAN International, as well as Procter & Gambel and Gillette and other large companies who wanted to use RFID to track goods and who believed an open standard was critical. The Auto-ID Center ceased to exist after October 2003. Today, EPCglobal operates as a not-for-profit joint venture set up by the Uniform Code Council to commercialize Electronic Product Code technologies developed by the Auto-ID Center and EAN International. *See Frequently Asked Questions (FAQs)*, RFID JOURNAL, http://www.rfidjournal.com/faq [hereinafter FAQs].

11. FINKENZELLER, *supra* note 9 at 2-7.

12. RFID tags are available in a variety of sizes; however all are relatively small which provides for their discrete character and practicality. Larger tags such as the hard anti-theft tags attached to merchandise in stores are easy to spot, whereas smaller tags—capable of bodily implantation—are no bigger than a grain of rice. Smaller still are tags which have been developed to be embedded within the fibers of national currency. EPIC, *supra* note 1. RFID chips can be as small as 0.3 millimeters square—about half the size of a grain of sand. *See Hitachi Unveils Smallest RFID Chip*, RFID JOURNAL, Mar. 14, 2003, http://www.rfidjournal.com/article/articleview/337/1/1/; *see also* Scott Granneman, *RFID Chips Are Here*, SECURITY FOCUS, June 26, 2003, http://www.securityfocus.com/columnists/169/.

13. FINKENZELLER, *supra* note 9, at 8.

14. ALAN BUTTERS, RADIO FREQUENCY IDENTIFICATION: AN INTRODUCTION FOR LIBRARY PROFESSIONALS 2 (2006), http://www.sybis.com.au/GeneratedItems/RFID%20Whitepaper.pdf.

15. FAQs, *supra* note 10.

16. *See How Does RFID Work*, RFID AND PRIVACY: A PUBLIC INFORMATION CENTER, http://rfidprivacy.mit.edu/access/how.html [hereinafter RFID and Privacy].

17. EPIC, *supra* note 1.

18. *Id.*

translates the received data, and stores it in a computer database.[19] Many factors affect the read range of RFID tags[20]

Overall, RFID in integrated technological system that requires all three components—tag, reader, and database—in order to operate. The hallmark of the system is its wireless feature which allows for the transmission of data via radio waves. This provides for a variety of benefits but also hosts limitations and for some, significant concern.

B. Limitations and Benefits of RFID

RFID was first developed during World War II as a means of recognizing the national origins of ships and planes,[21] but it was not until the 1980's that prices began to fall allowing government and private entities to develop more expansive uses of the technology.[22] Still, whereas a typical barcode costs less than one cent, the cost of an electronic RFID tag is currently between fifteen and sixty-five cents per tag[23] and will probably not become pervasive until the per chip costs equal to that of the barcode.[24] RFID readers pose an additional cost which varies depending on the level of wave frequency the reader is capable of intercepting.[25] Though companies require much fewer readers than individual tags, they still need thousands of readers to cover all their factories, warehouses and stores.[26]

Despite the relative expense of RFID as compared to other forms of Auto-IDs, the system has emerged as the front-runner due to its superior benefits in durability and specificity. Unlike bar codes, RFID tags do not require that a scanner or other devise to "see" the tag, but rather it can be read as long as the tag is within range of the reader.[27] This allows RFID tags to be read at a much greater distance than barcodes.[28] Additionally, the non line-of-sight characteristic of RFID tags means that the tags are not susceptible to exterior

19. FAQs, *supra* note 10; *see also* RFID and Privacy, *supra* note 16.

20. RFID tag read range maybe be affect by the frequency of operation; the power of the reader; interference from other RFID devices; the object tagged (e.g., tags on metal objects have a short read range than those on plastic objects); and the size and power of the antenna (though though it is practically impossible to build an antenna which will read tags from more than ten times the standard read range). *See* FAQs, *supra* note 10.

21. Meridith Levinson, *Successful Use of RFID Requires the Right Infrastructure*, CIO MAGAZINE, Dec. 1, 2003, http://www.cio.com/article/32004/Successful_Use_of_RFID_Requires_the_Right_Infrastructure.

22. Katherine Delaney, Note, *2004 RFID: Privacy Year in Review: America's Privacy Laws Fall Short with RFID Regulation*, 1 ISJLP 543, 548 (2005).

23. Larry Dignam, *RFID: Hit or Myth?*, BASELINE, Feb. 9, 2004, http://www.baselinemag.com/c/a/Intelligence/RFID-Hit-or-Myth/.

24. EPIC, *supra* note 1. Pricing for RFID tags is based on volume, the amount of memory of the tag, and packaging of the tag (e.g., whether it is encased in plastic or embedded in a label, etc.). *See* FAQs, *supra* note 10.

25. Low frequency readers can cost between $100 and $750, high frequency readers between $200 and $500, and ultra-high frequency readers between $500 and $2000. In addition, a $250 antenna costing is required. *See* FAQs, *supra* note 10.

26. *Id.*

27. *Id.*

28. ALBRECHT & MCINTYRE, *supra* note 3 at 37–53

damage such as rips and spills like bar codes, but rather may be embedded in packaging or encased in protective plastic for weatherproofing and greater durability.[29] Tags can also be read through most non-metallic substances (e.g., snow, fog, ice, dirt or paint). In fact, RFID systems boast a 99.8 percent or better success rate for unattended reading.

Another useful benefit of RFID is the degree of specificity that the technology permits. RFID tags have microchips that can store a unique serial number called an Electronic Product Code (EPC) for every product manufactured around the world as well as various other types of information.[30] EPC is a string of numbers and letters consisting of a header and three sets of data partitions. The first partition identifies the manufacturer, the second partition identifies the product type (e.g., stock keeping unit), and the third is the serial number of the unique item.[31] By separating the data into partitions, readers can search for items with a particular manufacturer's code or product code.[32] This allows companies to track each object independently, collect real-time data about each item, and store and act upon that information.[33] Standard bar codes which contain Universal Product Codes (UPCs) identify only the manufacturer and product, not the unique item.[34] For example, the bar code on a milk carton is the same as every other, making it impossible to identify which one might pass its expiration date first.[35] RFID, on the other hand, allows the shipper to track that particular carton of milk, allowing the retailer to access specific information such as when that carton of milk expires.[36]

These benefits are responsible for making RFID the primary means for keeping tabs on people, pets, products and vehicles.[37] RFID also helps to reduce administrative error, labor costs associated with scanning bar codes, internal (i.e., employee or customer) theft, errors in shipping goods, counterfeiting, mass recalls, inventory management and has even played a unique role in the U.S. government's efforts to combat terrorism.[38]

C. Current and Future Applications of RFID

RFID developers are creating more pervasive and potentially invasive uses of RFID as they refine the technology and as the price continue to decline.[39] The primary commercial and government application of the technology is to provide a tracking mechanism for the purposes of (1) inventory, (2) safety and security, and (3) consumer convenience. Each of these applications becomes

29. FAQs, *supra* note 10.
30. *Id.*
31. *Id.*
32. *Id.*
33. *Id.*
34. Delaney, *supra* note 22, at 543.
35. FAQs, *supra* note 10.
36. *Id.*
37. EPIC, *supra* note 1.
38. *Id.*
39. *Id.*

particularly controversial when used to track the buying habits, individual whereabouts, or to access other personally identifiable information.

1. Inventory

Inventory tracking is one of the principle applications of RFID. RFID systems enable business owners and government to have real-time access to inventory information thus streamlining their business process to ensure greater efficiency.[40] For example, studies show that products are not on store shelves seven percent of the time and retailers and manufacturers lose money every time a customer leaves a store without buying what they intended to purchase.[41] To avoid this, some companies have experimented with "smart shelves" which employ RFID to provide information as to exactly what products are on store shelves at any given time.[42] Companies that have used RFID in this way have achieved a significant degree of success.[43] Similarly, RFID can provide business owners a broader sense of a general and specific consumer buying habits by allowing data processing systems to read and compile information contained on the RFID tag of an item purchased by a specific consumer.[44]

Use of RFID to track warehouse goods has proven equally as effective. Companies position readers around the loading dock doors and on every bay. When a pallet of goods arrives, the reader on the dock door picks up its unique identification code. Computers then look up what product is using the EPC Network and inventory systems are alerted to its arrival. When the pallet is put in bay A, for example, the reader sends a signal saying item 1-2354-67890 is in bay A.[45] No unpacking, no handling, no barcode scanners required. Many companies have already employed RFID technology to track incoming goods.[46] Similarly, the Department of Defense has spent over $100 million over the last decade implementing RFID technology to track everything from rations to uniforms to tanks.[47] The goal of RFID implementation in the government has

---

40. *Id.*

41. FAQs, *supra* note 10.

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

43. In an academic study performed at Wal-Mart, RFID reduced instances of out of stock products by thirty percent for products selling between 0.1 and 15 units a day. *See* Bill Hardgrave, Mathew Waller & Robert Miller, *RFID's Impact on Out of Stocks: A Sales Velocity Analysis*, INFORMATION TECHNOLOGY RESEARCH INSTITUTE, Jun. 2, 2006, http://itrc.uark.edu/research/display.asp?article=ITRI-WP068-0606. Similarly, GAP has found that it can increase sales in RFID-equipped stores by seven to fifteen percent by freeing sales staff to spend more time with customers and less time in the stockroom. *See* Learning from Prada, RFID JOURNAL, June 24, 2002, http://www.rfidjournal.com/article/articleview/272; Staff Devices and Dressing Rooms for Prada, http://www.ideo.com/work/item/staff-devices-dressing-rooms/ (last visited April 1, 2009.

44. EPIC, *supra* note 1.

45. FAQ, *supra* note 10.

46. For example, the Boeing Company has successfully implemented RFID to track parts for its 787 Dreamliner aircraft. *See* Olga Kharif, *RFID's Second Wave*, BUSINESSWEEK, Aug. 9, 2005, http://www.businessweek.com/technology/content/aug2005/tc2005089_4131_tc_215.htm.

47. Alorie Gilbert, *RFID Goes to War*, C-NETNEWS.COM, Mar. 22, 2004,

been to prevent frontline troops from suffering supply shortages, as well as reducing the amount of lost, misplaced, and unused supplies.[48] Ultimately, the goal is to streamline the entire supply chain from manufacturing to distribution to the retailer.[49]

2. Safety and Security

RFID is currently used by the private and public sectors to improve safety and enhance security. One way RFID can be used to enhance individual safety is by tracking of pets,[50] inmates, and hospital patients[51] through either implanted or external RFID chips. RFID may also enhance consumer safety by using RFID to track and quickly recall defective products.[52] Finally, business and government have employed RFID as a mechanism for combating fraudulent practices.[53]

One of the most pervasive government uses of RFID in recent years as a means of enhancing safety and security is the use of the technology in passports.[54] Endorsed in 2004 by the International Civil Aviation Organization (ICAO), the international body responsible for passport standards[55] all U.S.

---

http://news.com.com/2008-1006-5176246.html; *but see* Booth-Thomas, *supra* note 7, at A8 (putting Department of Defense RFID spending at $272 million).

48. Gilbert, *supra* note 47; *see also* Harold Kennedy, *Army Trying to Expedite Flow of Supplies to Troops*, NATIONAL DEFENSE MAGAZINE, May 2001, http://www.nationaldefensemagazine.org/issues/2001/May/Army_Trying.htm (May 2001) ("Logistics is moving from a 'mass model' of dumping huge amounts of supplies into a combat theatre to a 'lean, agile delivery system focused on warfighter needs,' James T. Eccleston, assistant deputy undersecretary of defense for supply-chain integration, told the Quartermaster General's Symposium, in Richmond, Va.").

49. Jerry Brito, *Relax Don't Do It: Why RFID Privacy Concerns Are Exaggerated and Legislation is Premature*, 8 UCLA J.L. & TECH. 5, 4 (2004), http://www.lawtechjournal.com/articles/2004/05_041220_brito.pdf.

50. Cathy Booth Thomas, *supra* note 7, at A8.

51. Delaney, *supra* note 22, at 554.

52. For example, Michelin tires are now manufactured with a RFID tag embedded inside. This tag stores tire identification information which can then be associated with the vehicle identification number (VIN). *See* EPIC, *supra* note 1.

53. RFID used to combat drug counterfeiting in the pharmaceuticals industry. *See* Martin Downs, *Counterfeit Drugs: A Rising Public Health Problem*, WEBMD.COM, http://www.webmd.com/content/article/95/103346.htm; RFID used in currency as the European Central Bank is experimenting with RFID chips in euro notes. *See* Janis Mara, *Euro Scheme Makes Money Talk*, Wired News, July 9, 2003, http://www.wired.com/politics/security/news/2003/07/59565.

54. Electronic Passport, 70 Fed. Reg. 8305 (proposed Feb. 18, 2005) (codified at 22 C.F.R. pt. 51); RFID may also soon be used in driver's licenses or a national ID card as prescribed by the REAL ID Act of 2005, discussed *infra* at Section IV.A.1.

55. To ensure that U.S. e-passports are interoperable with other nations' systems, the document's embedded RFID chip will comply with specifications developed by the International Civil Aviation Organization (ICAO). The ICAO specification requires a minimum capacity of 32 kilobytes of memory for storing data on the chip, whereas the U.S. government has opted for a chip with 64 kilobytes of memory to allow for the potential storage of additional data or biometric indicators such as fingerprints or iris scans, sometime in the future. Before the department adds additional data or biometric identifier other than a digitized photograph, however, it says it will seek public comment through a new rule-making process. *See* Paul Price, *United States Sets Date for E-Passports*, RFID JOURNAL, Oct. 25, 2005, http://www.rfidjournal.com/article/articleview/1951/1/132/.

passports issued by the U.S. State Department after January 1, 2007 now have always-on radio frequency identification chips [56] as identified by a distinctive logo on the front cover of each RFID embedded passport.[57] These new passports contain the same information as a passport's data page including the passport holder's name, nationality, gender, date of birth, place of birth, passport number, issue date, expiration date, type of passport, and digitized photo.[58]

Use of RFID in passports has opened the possibility of a host of privacy concerns due to the sensitive nature of the information they provide. This is particularly worrying in light of the fact that the RFID chip used in e-passports permits chips to be read when placed within approximately 10 centimeters of an RFID reader.[59] To protect the sensitive information contained on the passport RFID chips, the government has established a number of security measures. First, to prevent skimming[60], the Department of State has added a shielding material to the passport's front cover and spine which ensures that the e-passport's RFID tag is unreadable as long as its cover is closed or nearly closed.[61] Additionally, the Department has implemented a system called Basic Access Control (BAC), which functions as a Personal Identification Number (PIN) in the form of characters printed on the passport data page.[62] Before a passport's tag can be read, this PIN must be inputted into an RFID reader.[63] The BAC also enables the encryption of any communication between the chip and reader.[64] While these safety and security features are perhaps the most beneficial uses of RFID, they are also the most controversial.

3. Consumer Convenience

RFID as a mechanism for facilitating convenience to the consumer is a third category of the technology's use. While RFID is currently used to prevent lost luggage[65] and facilitating library book check-out,[66] perhaps the greatest convenience to consumers is the employment of RFID to allow for contactless

---

56. *How to: Disable Your Passport*, WIRED NEWS, Jan. 2007, http://www.wired.com/wired/archive/15.01/start.html?pg=9.

57. *Id.*

58. Price, *supra* note 55.

59. *Id.*

60. "Skimming" is the act of creating an unauthorized connection with an RFID tag in order to gain access to its data. "Eavesdropping" is the interception of the electronic communication session between an RFID tag and an authorized reader. *Id.*

61. *Id.*

62. *Id.*

63. *Id.*

64. *Id.*

65. Delta Air Lines is testing a system that would embed RFID tags in the adhesive printed baggage labels to allow baggage tracking using RFID readers placed at strategic points such as luggage carousels. By using RFID, Delta hopes to be able to pinpoint a bag's location and automatically send a wireless message to a staff person in a position to pull the bag and send it to its proper destination. *See Delta Takes RFID under Its Wing*, RFID JOURNAL, June 20, 2003, http://www.rfidjournal.com/article/articleview/468; *see also* Bruce Mohl, *Radio Tags May Yet Solve the (Costly) Lost Baggage Problem*, BOSTON GLOBE, May 16, 2004, at M7.

66. Delaney, *supra* note 22, at 552.

payment transactions at retailers, toll booths, and public transit.

In 1997, ExxonMobil was the first to launch a contactless payment application known as "Speedpass".[67] Speedpass users are given a keychain fob with an embedded RFID tag that is programmed with a unique ID number and this number is associated with the user's payment information in Mobil's database, including credit card information.[68] Similarly, companies such as Mastercard and American Express, now offer contactless payment systems, respectively coined "PayPass" and "Express Pay". [69] In contrast to Exxon Mobil's Speedpass, credit cards that incorporate RFID technology, commonly referred to as "tap-and-go" or "smart" credit cards, can be used anywhere regular magnetic strip credit cards are accepted, as long the store has installed RFID readers.[70]

Contactless payment systems have been particularly successful with consumer transport. For example, U.S. highway toll booths across the country have implemented systems such as EZ-Pass to allow vehicles to seamlessly pass through tolls without stopping.[71] The tags are read remotely as vehicles pass through the booths and directly bill the toll to the user's account.[72] The system helps to speed traffic through toll plazas as it records the date, time, and billing data for the RFID vehicle tag.[73] Similarly, many public transit systems now issue payment cards embedded with RFID as a means of contactless fare payment. Using kiosks or direct deposit, commuters periodically add funds to their account, which is associated with the unique number in the RFID card.[74] Subway turnstiles and buses are equipped with RFID readers such that waving a card in front of them allows a passenger to pass through while deducting the appropriate fare from the user's account.[75]

The current and future uses of RFID are endless. Nevertheless, availability of such technology warrants a heightened level of responsibility, particularly in light of the potential threat to privacy posed by RFID.

III. PRIVACY IMPLICATIONS OF RFID

The movement to replace barcodes and magnetic strips with RFID tags on consumer goods and credit cards has raised a host of privacy concerns; principally, that business and government will link individuals' identities to

---

67. EPIC, *supra* note 1.

68. *Speedpass: How It Works*, http://www.speedpass.com/how/index.jsp (last visited April 1, 2009. To date, six million consumers have utilized the payment option at 7,500 Speedpass enabled locations. *See* EPIC, *supra* note 1.

69. *Wave the Card for Instant Credit*, WIRED NEWS, Dec. 14, 2003, http://www.wired.com/science/discoveries/news/2003/12/61603.

70. *Id.*

71. E-Z Pass Information: How it Works, http://www.ezpass.com/static/info/howit.shtml (last visited April 1, 2009).

72. *See generally* Delaney, *supra* note 22.

73. *Id.*

74. SmarTrip, http://www.wmata.com/fares/smartrip/ (last visited April 1, 2009).

75. *Id.*

uniquely numbered items and thereby track peoples' movements.[76] According to a study conducted by the Auto-ID Center at the Massachusetts Institute of Technology, 78 percent of respondents reported privacy concerns involving knowledge of what was being tagged or read with RFID systems.[77]

A. Anti-RFID Position

RFID critics argue that the benefits of company utility and consumer convenience do not outweigh the costs of infringement on privacy rights when personally identifiable information is linked to data collected by RFID systems. They argue that RFID tags in passports, credit cards, baggage, library books and various other consumer products could become tracking devices thereby creating an Orwellian world where retailers, law enforcement, and other unauthorized individuals could track persons simply by installing nearby readers.[78] To avoid this danger, many consumer groups are advocating for strict regulations or complete bans on RFID technology.[79]

Privacy experts have identified three technical aspects of RIFD tags that generate privacy concerns: they are promiscuous since they will talk to any compatible reader;[80] they are remotely readable since they can read at a distance through obtuse materials like cardboard, cloth, and plastic; and they are stealthy in that the tags are not only inconspicuous, but an individual remains unaware when and to whom the tags are transmitting information or when an unwanted third party is receipting tag information.[81] The direct consequence is that readers placed around the globe to constantly read, process, and evaluate consumer's behaviors and purchases and companies and government that retrieve information from tags can then potentially misuse and abuse the information received.[82] Additionally, if the tag is not disabled or if an individual were unaware that they were in possession of a tag, it would be possible to scan the RFID tag on the item from close range.[83] Other potential threats include workplace privacy where employers may require implanted or external RFID chips to track the activities of their employees.[84]

Those subscribing to this anti-RFID view believe that the solution to the privacy threat posed by RFID is to enact laws that will preempt any future

---

76. *See generally* Brito, *supra* note 49.

77. Levinson, *supra* note 21.

78. EPIC, *supra* note 1.

79. *Opponents of RFID include: Consumers Against Supermarket Privacy Invasion and Numbering (CASPIN); Electronic Privacy Information Center; Information Technology and Innovation Foundation.*

80. Some RFID readers have the capacity to read data transmitted by many different RFID tags such that if a person enters a store carrying several RFID tags, one RFID reader can read the data emitted by all of the tags, and not simply the signal relayed by in-store products. [epic.org] This capacity enables retailers with RFID readers to compile a more complete profile of shoppers than would be possible by simply scanning the bar codes of products a consumer purchases. See EPIC, *supra* note 1.

81. Price, *supra* note 58.

82. EPIC, *supra* note 1.

83. For example, in a product such as a watch, the antenna would have to be so small that the range would only be one foot. *See* FAQ, *supra* note 10.

84. *Id.*

problems that may arise out of the use of the technology. This idea was articulated by Paula J. Bruening of the Center for Democracy and Technology in a recent congressional hearing:

> It is more effective and efficient to begin at the outset of the development process to create a culture of privacy that incorporates sound technical protections for privacy and that establishes the key business and public policy decisions for respecting privacy in RFID use before RFID is deployed rather than building in privacy after a scandal or controversy erupts publically.[85]

Although some argue for an outright ban of RFID, most are satisfied with ensuring that measures are in place to mitigate any negative effects that might arise out of its use. One such measure is notification to and consent of the consumer so that they aware of the existence of an RFID tags and those tags are being read.[86] For example, EPIC encourages retailers to "introduce clear labeling and easy removal of tags to ensure that consumers receive proper notice of RFID systems and are able to confidently exercise their choice whether or not to go home with live RFID tags in the products they own."[87] In their view, an item traceable for an indefinite period of time crosses the line from utility to the company and infringement on privacy rights.[88] Finally, privacy advocates believe that consumers should have access to their personal information so that inaccurate information stored in RFID databases can be corrected and removed.[89]

B. Pro RFID Position

Those less critical of RFID have embraced what can be summarized as an "understand, not ban," campaign. Proponents of RFID stress that simply because a technology could be used in harmful ways does not mean it will[90] and that the current state of RFID is such that the benefits of the technology outweigh the potential risks.[91]

RFID advocates believe that preemption legislation restricting RFID technology acts as a solution to a yet unidentified problem which could lead to

---

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

86. *RFID and the Public Void, Hearing Before the California Legislature Joint Comm. on Preparting California for the 21st Century* (statement of Beth Givens, Privacy Clearinghouse Director), http://www.privacyrights.org/ar/RFIDHearing.htm#1.

87. ELECTRONIC PRIVACY INFORMATION CENTER, WORKING DOCUMENT ON DATA PROTECTION ISSUES RELATED TO RFID TECHNOLOGY, Jan. 19, 2005, http://www.epic.org/privacy/rfid/comments_art29.pdf.

88. Delaney, *supra* note 22, at 568.

89. *Id.*

90. Brito, *supra* note 49, at 13.

91. *Id.* (arguing that RFID is not as all-powerful as people claim and claims about RFID are exaggerated).

premature, unintended and perhaps unwanted consequences such as stunting the technology's development generally.[92] Instead of restrictive legislation, RFID proponents believe that the evolving nature of this new technology warrants freedom in allowing the market to dictate its development so as to allow unforeseeable future uses of the technology to come to fruition.[93] Market forces, therefore, are sufficient (at least for now) to meet consumer preferences on privacy.[94] Ultimately, RFID proponents find that whatever threats to privacy RFID currently poses is outweighed by the benefits such as business efficiency and convenience to the consumer.

RFID advocates stress that it is important to remember that public concern is with the access and control of data, not the technology itself and that there are already sufficient privacy protections in place. First, proponents of RFID claim that RFID restrictive legislation is redundant because federal and states laws protect individuals from collection and dissemination of their private information captured via RFID.[95] Second, it is practically impossible to build an antenna which will read tags from more than ten times the standard read range and most RFID chips cannot be tracked beyond an operating distance of about five feet.[96] Third, assuming individuals are aware of them, it is possible to disable RFID tags. For example, tags can be destroyed by rudimentary physical means such as microwaving or tapping with a hammer;[97] RFID radio waves can be easily detected and blocked;[98] and all readers and tags implement a kill command that permanently disables the tag.[99] Although it is not currently possible for a person to know when a tag they are carrying is being read, there have been significant advances in creating a device that is able to sense when tags you are carrying are being read.[100]

Groups have weighed in on both sides of the debate. As reflected in current RFID legislation, the pro-RFID position seems to be taking a greater hold.

IV. CURRENT RFID LEGISLATION

Katherine Albrecht, head of Consumers Against Supermarket Privacy Invasion and Number (CASPIAN) opined, "I think the main way we're going

92. *Id.*

93. *Id.* at 13.

94. *Id.* at 12.

95. *See infra* part V.B.

96. EPIC, *supra* note 1. However, this could change in the future.

97. *How to: Disable Your Passport*, *supra* note 56. However, destroying RFID tags in passports is not recommended, as passport tampering is punishable by up to 25 years in prison. *See id.*

98. FAQs, *supra* note 10. Blocker tags are available which allow for the obstruction of information gathered by RFID readers by simulating many ordinary RFID tags simultaneously. *See* EPIC, *supra* note 1.

99. EPIC, *supra* note 1; Some readers also implement other levels of this kill functionality such as "kill recycle", which destroys all information stored on the tag except for the information needed to recycle the tagged object. *See Id.*

100. *See* RFID Guardian, http://rfidguardian.org/index.php/Main_Page (last visited April 1, 2009).

to prevent RFID abuse is to limit its implementation."[101] To their distain, privacy activists seem to be losing the battle in the absence of a definitive push by law makers to regulate RFID. There is no federal legislation to date that regulates the technology, though there is federal legislation that promotes its use. At the state level, only 17 states have proposed RFID regulation legislation, with fewer states seeking to regulate RFID in 2007 than in 2006. To date, only four RFID regulating bills have passed through state Congresses and survived governor vetoes.[102]

A. Federal RFID Legislation

1. The REAL ID Act of 2005

As part of its counterterrorism efforts, Congress passed the "REAL ID Act of 2005."[103] Title II of the Act—"Improved Security for Driver's License' and Personal Identification Cards"—acts as a federal mandate for state-issued drivers licenses and identity cards.[104] In addition to proscribing minimum documentation requirements such as the type of information that must be contained in the documents, § 202(b)(9) of the Act requires that all IDs employ "a common machine-readable technology, with the defined minimum data elements", namely, RFID.[105] Included in this is the use of RFID in U.S. passports which has now been fully implemented by the federal government.

So far there has been strong opposition from the states in implementing the REAL ID standards. While states had until March 31, 2008 to adopt the provisions of the Act or ask for an extension, at least four states have expressly rejected the system.[106] However, such opposition stems more from a state's rights stance rather than a concern for individual privacy. The mere fact that

---

101. Hiawatha Bray, *Usefulness of RFID Worth the Annoyance*, BOSTON GLOBE, Apr. 12, 2004, at D2.

102. *See infra* part IV.B.

103. REAL ID Act was enacted as Division B of the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, Pub. L. 109-13, 119 Stat. 231 (2005).

104. Real ID Act of 2005, Pub. L. No. 109-13, Division B, 119 Stat. 231, 302 (2005) (codified in scattered sections of 8 U.S.C.).

105. The statute reads:

> *Minimum document requirements*: To meet the requirements of this section, a State shall include, at a minimum, the following information and features on each driver's license and identification card issued to a person by the State:
>
> (1) The person's full legal name.
>
> (2) The person's date of birth.
>
> (3) The person's gender.
>
> (4) The person's driver's license or identification card number.
>
> (5) A digital photograph of the person.
>
> (6) The person's address of principle residence.
>
> (7) The person's signature.
>
> (8) Physical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purposes.
>
> (9) A common machine-readable technology, with defined minimum data elements.

106. To date, nineteen states have rejected the Real ID Act. *See* Electronic Privacy Information Center, National ID Cards and Real ID Act, http://epic.org/privacy/id-cards/#state (last visited April 1, 2009).

such proscriptive federal RFID legislation has been passed indicates that to a certain extent, Americans have embraced the technology making future state bans on RFID unlikely.

2. RFID Right to Know Act

CASPIAN proposed a bill in 2003 titled the "RFID Right to Know Act of 2003."[107] This proposed piece of federal legislation would amend several portions of the U.S. Code including the addition of an RFID specific subchapter to 15 U.S.C., Chapter 94 on privacy.[108] Considering the passage of the REAL ID Act, it is unclear whether a federal law restricting the use of RFID will be implemented in the near future.

B. State RFID Legislation

The majority of RFID regulatory activity has been proposed at the state level. In 2005, twelve states introduced RFID-related legislation.[109] In 2006, at least seventeen states introduced privacy bills regulating RFID.[110] California and Rhode Island each vetoed RFID-related bills,[111] while Wisconsin and New Hampshire became the first two states to enact RFID-related legislation.[112] Most recently, privacy bills regulating RFIDs were introduced in at least thirteen state legislatures in 2007 with both California and North Dakota enacting legislation.[113]

Proposed RFID legislation at the state level has typically targeted five different issues:[114] disclosure requirements;[115] tag removal or deactivation requirements;[116] prohibition on the linking of RFID data to personal

---

107. Consumers Against Supermarket Privacy Invasion and Numbering, RFID Right to Know Act of 2003, *available at* http://www.nocards.org/rfid/rfidbill.shtml (last visited April 1, 2009).

108. Mark Baard, *Lawmakers Alarmed by RFID spying*, WIRED NEWS, Feb. 26, 2004, http://www.wired.com/politics/security/news/2004/02/62433.

109. National Conference of State Legislatures, 2005 Privacy Legislation to Radio Frequency Identification (RFID), *available at* http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/RadioFrequencyIdentificationLegislation2005/tabid/13451/Default.aspx (last visited April 1, 2009).

110. National Conference of State Legislatures, 2006 Privacy Legislation to Radio Frequency Identification (RFID), *available at* http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/RadioFrequencyIdentificationLegislation2006/tabid/13464/Default.aspx (last visited April 1, 2009).

111. *Id.*

112. *Id.*

113. National Conference of State Legislatures, 2007 Privacy Legislation to Radio Frequency Identification (RFID), *available at* http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/RadioFrequencyIdentificationLegislation2007/tabid/13456/Default.aspx (last visited April 1, 2009).

114. *C.f.* UTAH CODE ANN § 76-6-702 & 76-6-703 (West 2005) (clarifying that computer crimes laws apply to wireless networks, but exempting from the Computer Crimes Act certain collections of information through the use of RFID-type technology).

115. State bills generally seek requirements that would encourage notice for consumers. *See, e.g.*, RFID Right to Know Act of 2005, S.B. 638, 93rd Gen. Assemb., 2d Reg. Sess. (Mo. 2006).

116. If people know that an RFID tag exists and have the option to disable it, then they are in a position to control whether they want to utilize the technology. *See, e.g.*, Radio Frequency Identification Tag Control Act, H.B. 314, 1st Sub., 2004 Gen. Sess. (Utah 2004).

information;[117] prohibition of specific RFID-related uses;[118] and establishment of research and recommendations committees.[119] Enacted restrictive RFID legislation to date has involved requiring disclosure, regulating specific, extreme cases of RFID as well as laws insisting upon further research of the technology.

Only four of the seventeen states that have proposed RFID-related legislation have enacted laws regulating the technology in some way. In three of the four states that have enacted laws—Wisconsin, North Dakota and California—RFID is regulated only in one specific extreme circumstance, namely, forced bodily implementation of an RFID chip.[120] In the fourth state, New Hampshire, the regulation of RFID pertains to a less dramatic (and probably more realistic) scenario. Although subject to exceptions, New Hampshire Revised Statutes § 236:130 prohibits the use of surveillance devices, including RFID, to identify ownership of a vehicle or the identity of a vehicle's occupants.[121] New Hampshire also passed another bill that establishes a commission on the use of RFID, which was required to report its findings and any recommendations for legislation by November 1, 2007 and submit a final report before dissolving on November 1, 2008.[122] Rhode Island's state legislature has also passed legislation regulating RFID; however, each time the bills have been vetoed by the governor.[123]

V. THE FUTURE OF RFID LEGISLATION

Despite the proliferation of privacy advocacy groups as well as state legislative proposals, the public appears to be relatively uninterested in RFID legislation. Assuming legislative enactment is an accurate measure of public opinion, of the relatively few proposed restrictive state bills have failed while proscription RFID-related legislation such as the REAL ID Act has achieved at least some success. Additionally, in a study of 8500 adults conducted in April 2005, only 41 percent of those questioned had even heard of RFID

117. *See, e.g.*, S.B. 1834, 2003-2004 Session (Cal. 2004) (outlining when it is permissible to use or record personally identifiable information in the context of an RFID transaction).

118. *See* WIS. STAT. § 146.25 (2009) (making it illegal to implant an RFID tag in an individual); N.D. CENT. CODE § 12-1-5 (2009) (same); CAL. CIV. CODE § 52.7 (West 2009) (same); N.H. REV. STAT. ANN. § 236:130 (2009) (making it illegal to use RFID tags to determine the ownership of a motor vehicle or to determine the occupants within a motor vehicle).

119. *See, e.g.*, 2006 N.H. Laws Chapter 165 (establishing a Commission on the Use of Radio Frequency Technology).

120. *See supra* note 118.

121. *Id.*

122. *See supra* note 119.

123. *See* H5929, Gen. Assemb., Jan. Sess. 2005 (R.I. 2005) (prohibiting the use of RFID by state or municipal agencies for tracking the movement or identity of an employee, student or client as a condition of obtaining a benefit or services) (vetoed July 15, 2005); H7432, Gen. Assemb., Jan. Sess. 2006 (R.I. 2006) (prohibiting use of RFID by state and local governments in tracking movement or identity of employees, students, or clients; or as a condition for obtaining benefits or services as well as providing civil action as and exceptions for requirements of federal law, department of corrections, and emergency medical care) (vetoed June 23, 2006); S2668, Gen. Assemb., Jan. Sess. 2006 (R.I. 2006) (same) (vetoed June 23, 2006).

technology.[124] Of those surveyed, 65 percent were concerned about privacy issues, including 25 percent that were "very concerned."[125] Interestingly, adults who knew more about RFID technology were actually less concerned about privacy issues than those who had not heard of RFID.[126] While there is some resistance to certain privacy restricting measures,[127] these concerns are not generating a national public outcry. Three factors can be identified as to contributing to the general apathy and acceptance of RFID among American consumers: (1) ease, convenience, and productivity; (2) perception of legal safeguards; (3) post-9/11 societal value changes regarding privacy.

A. Ease, Convenience, and Productivity

The advancement in technology has created an environment where anyone can acquire data about another individual through public records and other sources. For example, "paying just $26 for each, the Foundation [for Taxpayer and Consumer Rights] obtained the [social security numbers] and home addresses of CIA Director George Tenet, Attorney General John Ashcroft, and Presidential Chief Political Advisor Karl Rove"[128] yet the public as a whole does not seem to care. In fact, consumers routinely offer their personal information willingly, particularly to retailers who often then sell the information to a third party.[129]

Apparent public apathy toward personal privacy seems to stem in part from the ease, convenience and heightened productivity that technological advances seem to provide. As previously discussed, consumers receive numerous benefits from RFID to better facilitate their fast-paced lives including contactless "tap-and-go" credit cards, toll booth passes, and mass transit payment cards. Additionally, increased efficiency and productivity in the supply chain provides greater supply at retail and grocery stores which amounts to not only greater selection choice, but also lower prices for consumers. Finally, while one's privacy is threaten by the potential risk that personal information contained on an RFID chip is captured by an unauthorized party, RFID in passports and other identification also enhances

124. Collins, *supra* note 4.

125. *Id.*

126. *Id.*

127. The Washington Metropolitan Area Transit Authority was forced to amend its privacy policy to limit access to collected personal information after consumers complained of the implementation of SmarTrip cards to use Metro parking garages that required users to identify who they were and where they were traveling in order to have access to transportation. *See* Open Letter from Cedric Laurant, Policy Counsel for the Electronic Privacy Information Center, regarding Washington Metropolitan Area Transit Authority's Proposed Amendments to the Public Access to Records Policy, *available at* http://www.epic.org/open_gov/foia/wmata/parp_cmts-021405.html (last visited April 1, 2009).

128. Harry A. Valetk, *Mastering the Dark Arts of Cyber Space: A Quest for Sound Internet Safety Policies*, 2004 STAN. TECH. L. REV. 2, n.161 (2004) (citing *Group Gets Private Data on Tenet, Ashcroft to Underscore Need for Tougher Laws*, USATODAY.COM, Aug. 29, 2003, *available at* http://www.usatoday.com/tech/news/internetprivacy/2003-08-28-privacy-tenet_x.htm).

129. Delaney, *supra* note 22 at 548 (stating "retailers may offer incentives to have consumers to sign off on the kill provision, authorizing disclosure to third parties").

security and theft protection by ensuring the correct person is in possession of the document.

B. Perception of Legal Safeguards

Most privacy protections that consumers have acquired have been through statutes or industry standards.[130] While they may not in fact be adequate to regulate privacy violations created by RFID, the public perception that structural legal safeguards already exist contributes to their complacency to enact specific RFID restrictive legislation since they seem redundant.

1. Federal Constitutional and Statutory Provisions

Although there is no explicit federal right to privacy in the United States, there is a perception that privacy rights exist under federal law, particularly since Courts have interpreted certain areas such as sexual and reproductive rights as deserving protection under the U.S. Constitution.[131] Rather than a uniform and comprehensive privacy law, a variety of federal and state laws are available for data protection.[132] Federal laws relevant to RFID privacy protection include (1) the Fourth Amendment of the Constitution, (2) the Privacy Act, (3) Electronic Communications Privacy Act (ECPA), and (4) the Identity Theft and Assumption Deterrence Act (ITADA).

a. Fourth Amendment

The Constitution arguably provides limited privacy protections. The Fourth Amendment states,

> 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.[133]

The purpose of the Fourth Amendment was "to prevent the use of governmental force to search a man's house, his person, his papers and his effects,"[134] but "cannot be translated into a general constitutional 'right to privacy'."[135] Fourth Amendment jurisprudence has adopted a two-prong

---

130. Valetk, *supra* note 128, at n.156.

131. *See* Lawrence v. Texas, 539 U.S. 558 (2003); Roe v. Wade, 410 U.S. 113 (1973); Griswold v. Connecticut, 381 U.S. 479 (1965).

132. Eric Dash, *Strong Privacy Laws May Explain Data Security in Europe*, INTERNATIONAL HERALD TRIBUNE, Aug. 8, 2005, *available at* http://www.iht.com/articles/2005/08/07/news/data.php (last visited April 1, 2009).

133. U.S. CONST. Amend. IV.

134. Olmstead v. United States, 277 U.S. 438, 463 (1928).

135. Katz v. United States, 389 U.S. 347, 350 (1967); *see also id.* at 350 n.5 (discussing other amendments that protect privacy: First Amendment, "freedom to associate and privacy in one's associations"; Third Amendment, no quartering of soldiers; and Fifth Amendment, the right to a "private enclave where he may lead a private life"). Later, in *Griswold v. Connecticut*, the Court also

approach: whether the action taken was a "search", and, if such action was a search, whether the search was unreasonable.[136] Under this reasonableness test, a search occurs when sense-enhancing technology obtains information "that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area," and that the technology used "is not in general public use."[137]

Radio frequency tracking has been established as a qualifying search mechanism under the Fourth Amendment; however, privacy protections are nevertheless limited. First, police use of RFID technology to merely augment their five senses and track people would not be a "search" under the Fourth Amendment and would therefore be permissible.[138] Second, searches conducted in public afford no privacy protection. In *Knotts*, the Court found radio frequency tracking conducted in public was not a violation of the Fourth Amendment since there is no reasonable expectation of privacy when traveling in an automobile on public roads.[139] By contrast, searches within a constitutionally protected space such as a home do require protection.[140] Finally, the Fourth Amendment does not protect actions by non-governmental officials. In *United States v. Jacobson,*[141] the Court concluded that the Fourth Amendment applies only to government action,[142] and not to action by private individuals, no matter how reasonable.[143] Accordingly, a Wal-Mart employee could sell products with RFID tags,[144] fail to disable the tags at the point of sale,[145] follow customers home, and use an RFID reader (from outside the house) to retrieve various information on the products in their home. Due to these limitations, the Fourth Amendment may be effective in regulating government's use of RFID, but not RFID use by the private sector.

b. Privacy Act of 1974

The Privacy Act of 1974 ("Privacy Act" or "Act")[146] is the most comprehensive U.S. law pertaining to privacy.[147] Like the Fourth Amendment,

---

found "zones of privacy" in the penumbras and emanations of the Ninth Amendment. 381 U.S. at 484.

136. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

137. Kyllo v. United States, 533 U.S. 27, 34 (2001).

138. United States v. Knotts, 460 U.S. 276, 282-83 (1983).

139. *Id.* at 281-82 (*citing Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

140. In *Kyllo*, the Court held that the use without a warrant of a thermal imaging device to scan the level of heat emanating from within a home constituted an unreasonable search under the Fourth Amendment. 533 U.S. at 34.

141. 466 U.S. 109 (1984).

142. This includes private individuals acting as an agent of the government or with the participation or knowledge of the government. *See id.* at 113.

143. *Id.*

144. *See* WYLD, *supra* note 6, at 19.

145. Disabling, or "killing" an RFID tag involves using an electromagnetic pulse to destroy the circuits of the chip. *See* Jonathan Collins, *RFID-Zapper Shoots to Kill*, RFID JOURNAL, Jan. 23, 2006, http://www.rfidjournal.com/article/articleview/2098/1/1/.

146. 5 U.S.C. § 552a(2006).

147. John M. Eden, *When Big Brother Privatizes: Commercial Surveillance, The Privacy Act of 1974, and the Future of RFID*, 2005 DUKE L. & TECH. REV. 20, ¶ 4 (2005).

the Privacy Act does not apply to private entities; rather, it only applies to government agencies or government-controlled corporations, such that private corporations are not bound by the fair information practices, open-access rules, and data-ownership principles embodied in the Act.[148] Additionally, the Privacy Act provides citizens a right to review private information collected by government agencies,[149] and a right to correct misinformation.[150] Again, these rights do not apply to activities by private entities.

It is important to note that the Privacy Act does not take effect until data or other information has been collected; that is, the Act does not prevent data collection, but rather data misuse.[151] According to the Government Accountability Office, "the Privacy Act is likely to have a limited application to the implementation of RFID technology because the Act only applies to the information once it is collected, not whether or how to collect it."[152] That said, it is important to remember that privacy violations really only occur once the data is misused. While possessing data might lead to abuse, it does not necessarily create a harm.

c. Electronic Communications Privacy Act (ECPA)

The Electronic Communications Privacy Act (ECPA)[153] provides a number of important regulations for electronic communications, including a general bar against peddling personal information intercepted through electronic transactions such as contact-less transmissions.[154] The ECPA makes it a crime for any person who, "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[155] If a radio frequency transmission from an RFID tag is deemed "communication" under the Act, it may be protected under the ECPA.

The ECPA is limited in a number of ways. First, the Act applies only to the contents of communications; transactional records can lawfully be disclosed, even sold, so long as the purchaser is not the federal government.[156] Therefore, the EPCA likely could not prevent companies from gathering and sharing transactional data transmitted from RFIDs.

---

148. 5 U.S.C. § 552a(a)(1).

149. 5 U.S.C. § 552a(d)(1).

150. 5 U.S.C. § 552a(d)(2)-(3).

151. James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1474 (2004) (pointing out that while "[t]he Privacy Act does include a provision that extends its coverage to databases created under government contract," this particular provision, "does not include governmental searches of private sector databases already compiled and maintained for other purposes").

152. *See* Jerry Klang, *Informational Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1231-32 (1998) (arguing that the Privacy Act, and other omnibus privacy statutes, utterly fail to protect data privacy because "they apply only to government action").

153. 18 U.S.C. §§ 2510-2522 (2006).

154. 18 U.S.C. § 2511(1)(c)-(d)

155. 18 U.S.C. § 2511(1)(a).

156. 18 U.S.C. § 2703(c)(1)(A).

d. Fair Credit Reporting Act (FCRA)

The Fair Credit Reporting Act (FCRA)[157] may have limited application to RFID, even though the Act was designed for a purpose completely unrelated to RFID transmissions.[158] Additionally, the FCRA does not constrain what third party payment providers can do with sensitive consumer information.[159] Consequently, Courts have consistently held that sensitive consumer information can be exchanged with impunity so long as a "legitimate business interest" can be identified.[160] Still, there may be an RFID regulatory mechanism under the FCRA if private actions do not rise to the level of a legitimate business interest.

e. Identity Theft and Assumption Deterrence Act (ITADA)

The Identity Theft and Assumption Deterrence Act (ITADA)[161] makes identity theft a federal crime, and is perhaps the strongest existing federal law in regulating private sector usage of RFID. Under 18 U.S.C. §(a)(7), "means of identification" does not require the production, possession, or use of an actual identification document. A RFID tracking number of a particular item could be used as a "means of identification" under this statute, thereby making possession of such information a federal crime.

2. State Statutory Provisions

As previously discussed, no state has enacted an overall ban on RFID technology.[162] Consumers are not void of protection, however, since many states have specific privacy laws in place that protect consumer privacy regardless of the form of technology used to violate it. California will be discussed here by way of example since its privacy laws reflect many other state jurisdictions and are most likely to provide RFID protections.

Unlike the federal Constitution, ten state constitutions explicitly recognize the right to personal privacy.[163] In California, the provision is self-executing and confers an individual right of action against the government intrusion into the personal lives of citizens as well as protecting against business's misuse of personal information.[164] More specific to RFID, the California Supreme Court

157. 15 U.S.C. §§ 1681-1681x (2006).

158. *See generally* Eden, *supra* note 147; *see also* 15 U.S.C. § 1681 (explaining congressional findings and statement of purpose).

159. 15 U.S.C. § 1681b(a)(3)(F).

160. Oscar H. Gandy, Jr., *Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace*, 1996 U. Chi. Legal F. 77, 80 (1996).

161. Pub. L. No. 105-318, 112 Stat. 3007 (1998) (to be codified in scattered sections of 18 & 28 U.S.C.).

162. Only specific uses of the RFID technology are banned in Wisconsin, New Hampshire, North Dakota, and California. *See supra* note 118.

163. ALASKA CONST. art. I, § 22; ARIZ. CONST. art. II, § 8; CAL. CONST. art. I, § 1; FLA. CONST. art. I, § 23; HAW. CONST. art. I, § 6; ILL. CONST. art. I, §§ 6 & 12; LA. CONST. art. I, § 5; MONT. CONST. art. II, § 10; S.C. CONST. art. I, § 10; WASH. CONST. art. I, § 7.

164. *See* White v. Davis, 522 P.2d 222, 234 (Cal. 1975).

in White v. Davis[165] found that the main purpose of the constitutional grant of privacy is to tackle "the accelerating encroachment on personal freedom and security caused by increased surveillance and date collection activity in contemporary society."[166] Citing legislative history, the Court explained that the constitutional amendment was meant to address concerns such as the "[c]omputerization of records [that] makes it possible to create 'cradle-to-grave' profiles of ever American," as well as the race to compile ever more "extensive sets of dossiers of American citizens."[167]

In addition to constitutional provisions, other state laws may provide sufficient protection against RFID privacy intrusions. For example, California, like most jurisdictions, recognizes common law privacy torts.[168] The abuse of RFID tracking might be covered by the tort for unreasonable intrusion upon the seclusion of another if there is an intentional intrusion upon the solitude or seclusion of another[169] and the intrusion is one that would be "highly offensive to a reasonable person."[170] However, this tort generally does not apply to publicly known individuals.[171]

3. Industry Regulation

Industry self-regulation of RFID is a third way that consumers' privacy may be protected. These regulations and guidelines are provided by a variety of sources including the International Organization for Standardization (ISO), EPCglobal, the Federal Communications Commission (FCC), the Federal Trade Commission (FTC), and organizations such as the ACLU who signed the 2003 "Joint Statement", yet all possess inherent limitations.

a. International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) has adopted standards for some very specific applications of RFID (e.g., tracking animals, smart cards, etc.) which require encryption to keep data secure.[172] Unfortunately, industry standards are lacking in covering the use of personal information.[173]

---

165. *Id.*

166. *Id.* at 233.

167. *Id.*

168. *See, e.g.*, Shulman v. Group W Productions, Inc., 955 P.2d 469 (Cal. 1998).

169. Here, solitude does not depend on the victim's location, but rather on the victim's expectation of privacy and the kind of invasion that took place. *See* Restatement (Second) of Torts § 652B cmt. c; *see also* Med. Lab. Mgmt. Consultants v. Am. Broad Cos., 306 F.3d 806, 812-13 (9th Cir. 2002).

170. RESTATEMENT (SECOND) OF TORTS § 652B (1977). Whether the information is publicized is irrelevant for this tort. Liability depends solely upon whether the individual's solitude was interrupted upon. *Id.* at § 652B cmt. a.

171. *Id.* § 652B cmt. c.

172. FAQs, *supra* note 10.

173. Delaney, *supra* note 22, at 566.

b. EPCglobal

EPCglobal has released a set of guidelines for use of electronic product codes (EPC) on consumer products.[174] Guidelines on EPC for Consumer Products issued by EPCglobal highlights four principles to guide the development and use of RFID technology: security, consumer notice, consumer choice, and consumer education.[175] Security refers to the proper use, storage, protection of consumer data, both on the aggregate and individual level to protect data to the full protection of state and federal law.[176] Consumer notice is achieved by clear, conspicuous and effective labeling of all products that contain an item-level RFID tag such that consumers can make an educated choice.[177] Consumer choice suggests that consumers must be given the option to "kill" or discard the RFID tag at the point of sale with no negative consequences.[178] Finally, consumer education ensures that consumers are aware of the potential negative effects of RFID technology.[179]

c. Federal Communications Commission (FCC)

The Federal Communications Commission (FCC) has also provided some guidance on the use of RFIDs.[180] Restrictions can be place on RFID under the FCC since RFID tags transmit signals using bandwidth.[181] For example, 47 C.F.R. § 15.240 restricts the use of the tags to "commercial and industrial areas."[182] In general, the FCC helps to restrict any covert collection of data using RFID technology by requiring those permitted to use RFID systems notify the Office of Engineering and Technology of locations of any RFID-related devices.[183]

d. Federal Trade Commission (FTC)

The Federal Trade Commission (FTC) has played a significant role in educating the public of RFID and as a forum for discussion,[184] but a limited

174. Guidelines on EPC for Consumer Products, http://www.epcglobalinc.org/public/ppsc_guide/ (last visited April 1, 2009).

175. *Id.*; *see also* Your Privacy: P&G Position on Electronic Product Coding (EPC): Public Statement from the Proctor & Gamble Company Regarding EPC Usage, http://www.pg.com/company/our_commitment/privacy_epc/epc_position.shtml.

176. Guidelines on EPC for Consumer Products, *supra* note 174.

177. *Id.*

178. David J. Warner, *A Call to Action: The Fourth Amendment, The Future of Radio Frequency Identification, and Society*, 40 LOY. L.A. L. REV. 853, 877(2005).

179. Guidelines on EPC for Consumer Products, *supra* note 174.

180. Delaney, *supra* note 22, at 561.

181. *Id.*

182. Intentional Radiators Radiated Emission Limits, Additional Provisions, 47 C.F.R. § 15.240 (2009).

183. *Id.* at §15.240(f).

184. The Federal Trade Commission hosted a one-day conference on RFID at which all sides of the debate gathered to participate. *See* Federal Trade Commission, Radio Frequency Identification: Applications and Implementation for Consumers, http://www.ftc.gov/bcp/workshops/rfid/.

role in its regulation. While the Privacy Rights Clearing House has voiced its concern and has requested that the Federal Trade Commission (FTC) regulate the use of RFID,[185] the FTC disagrees. A report by the FTC states that the main protectors of privacy rights should be industry participants, not federal legislators or regulators.[186]

e. Joint Statement

In November 2003, a coalition of thirty-five organizations, including the ACLU, EFF, and EPIC, released a position paper on RFID know as the "Joint Statement."[187] The Joint Statement calls for not only a public dialog of the privacy rights implications of RFID, but also ask industry to impose a voluntary moratorium on item-level tagging until a "formal technology assessment" sponsored by a "neutral entity" is completed.[188]

The Joint Statement lists several "RFID practices that should be flatly prohibited"[189] including that "merchants must be prohibited from forcing or coercing customers into accepting. . .RFID tags in the products they buy."[190] Since forcing or coercing persons into doing anything against their will is already tortious conduct, the EPIC has proposed a series of RFID guidelines issued by the EPIC better explain how privacy advocates define "force". Namely, merchants shall not "[c]oerce individuals to keep tags turned on after purchase for such benefits as warrantee tracking, loss recovery, or compliance with smart appliances."[191]

C. Post 9/11 Changed Social and Cultural Values Regarding Issues of Privacy

Americans are admittedly concerned with privacy protection, despite evidence of public complacency toward RFID. A UPI-Zogby International poll conducted on April 03, 2007 found that 85 percent of respondents said privacy of their personal information is important to them as consumers.[192] Nevertheless, other forces such as the War on Terror have likely made some impact on the way Americans manage their privacy concerns in practice.

---

185. *RFID 101*, RFID GAZETTE, June 28, 2004, http://www.rfidgazette.org/2004/06/rfid_101.html.

186. Mark Willoughby, *Securing RFID Information*, COMPUTERWORLD, Dec. 20, 2004, http://www.computerworld.com/s/article/96051/Securing_RFID_information.

187. Albrecht et al., *RFID Position Statement of Consumer Privacy and Civil Liberties Organizations*, Nov. 2003, http://www.privacyrights.org/ar/RFIDposition.htm [hereinafter RFID Position Statement].

188. *Id.*

189. *Id.*

190. *Id.*

191. *Id.*

192. Electronic Privacy Information Center, Public Opinion on Privacy, http://epic.org/privacy/survey/#polls.

1. Pre-9/11

Traditionally, Americans have tended to not trust government to protect privacy, but trust corporations.[193] This mentality is reflected in the various federal privacy laws such as the Fourth Amendment and the Privacy Act which apply to government, but not to private entities.[194] Additionally, efforts at the federal,[195] state,[196] and local[197] level to adopt opt-in privacy standards for personal data have often failed. This is in direct contrast to the European mentality which trusts a democratically elected government before big business. In effect, the United States has tended to view privacy as a consumer and economic issue whereas Europe regards privacy as a fundamental right.[198]

The legal consequence of the American mentality is that privacy oversight in the United States is decentralized. Data protection is not the core mission of any government agency and there are more laws restricting the government collection and use of information such as the Fourth Amendment.[199] By contrast, American businesses are treated as individuals and therefore given relatively free rein to collect and sell a consumer's personal information.[200] In addition, Americans tend to be more willing to give up their information to a business entity.[201] This is in spite of the fact that data security has been on the minds of many Americans as numerous companies such as Bank of America, Citigroup, Ralph Lauren Polo, and Boeing have announced data breaches in recent years which have resulted in compromised account numbers, social security numbers, address, and other personally identifiable information.[202]

---

193. Dash, *supra* note 132.

194. See *supra*, part IV.A.

195. For examples of general opt-in legislation at the federal level, *see* Consumer's Right to Financial Privacy Act, H.R. 2720, 107th Cong. (2001); Privacy Act of 2001, S. 1055, 107th Cong. (2001); Unsolicited Commercial Electronic Mail Act of 2001, H.R. 718, 107th Cong. (2001); Online Personal Privacy Act, S. 2201, 107th Cong. (2001); Financial Institution Privacy Protection Act of 2001, S. 450, 107th Cong. (2001); Consumer Online Privacy and Disclosure Act, H.R. 347, 107th Cong. (2001); Unsolicited Commercial Electronic Mail Act of 2001, H.R. 95, 107th Cong. (2001).

196. For examples of proposals at the state level, *see* S.B. 1258, 45th Leg., 2d Sess. (Ariz. 2002); Financial Privacy Protection Act of 2002, A.B. 1775, 2001-02 Reg. Sess. (Cal. 2002); H.F. 285, 79th Gen. Assemb., 1st Sess. (Iowa 2001); Consumer Privacy Act, S.B. 2988, 224th Leg. Sess. (N.Y. 2001); Consumer Internet Privacy Act, S.B. 4402, 224th Leg. Sess. (N.Y. 2001); S.B. 1547, 48th Leg., 2d Sess. (Okla. 2001).

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

198. Dash, *supra* note 132.

199. *Id.*

200. *Id.*

201. *Id.* "Ask a French person their phone number, and they will ask you why; American's don't ask why at all." *See id.*

202. *Id.*

2. Post 9/11

The events of September 11, 2001 changed the world overnight, including the way Americans balance the principles of privacy and security. As Senator Patrick Leahy noted, "In our constitutional system, there is always tension between liberty and security—and never more than since September 11th."[203] The way Americans chose to resolve this tension is to place greater trust in government.

Since 9/11, Americans seem have continued their pro-corporation stance by continuing to trust corporations with personal information as has traditionally been the case. While the public may be critical when particular breaches of personal information occur, overall, Americans continue to trust the private sector with their private information.

The noticeable change in American attitudes is a greater trust in government as a means of protecting individuals from acts of terror and other threats of violence. Such security measures, however, are at the expense of personal privacy—a trade that Americans seem comfortable in making. Curiously, critics of RFID continue to focus on private uses of the technology, and mention threats from the government only in passing.[204]

Immediately after the September 11, 2001 terrorist attacks, many Americans reported greater trust in government, and that even mere criticism of the government was inappropriate.[205] Polls showed that Americans were willing to accept more invasive police surveillance technologies such as facial recognition and greater collection of biometric identifiers.[206] As recent as 2007, a UPI-Zogby International poll conducted on April 13-16, 2007 asked 5,932 U.S. residents whether the U.S. government should be allowed to suspend privacy laws to share terror information.[207] Only slightly more than half (53 percent) said they are against the government having the ability to temporarily suspend federal privacy laws to enable agencies to better share counter-terrorism information, including the personal data of American citizens.

Assuming enacted legislation (or lack thereof) is another accurate indicator of public opinion, legislation enacted post 9/11 seems to demonstrate the willingness of individuals to trade personal liberties for security. For example, as an immediate response to the September 11 attacks, Congress drafted the USA PATRIOT Act, a mammoth piece of anti-terrorism legislation that they quickly signed into law less than a month later.[208] According to the Electronic Frontier Foundation, the PATRIOT Act "broadly expands law enforcement's surveillance and investigative powers and represents one of the most

---

203. Leahy, *supra* note 2.

204. Brito, *supra* note 49, at 11.

205. Electronic Privacy Information Center, Public Opinion on Privacy, http://epic.org/privacy/survey/#polls.

206. *Id.*

207. *Id.*

208. Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub L. No. 107-56, 115 Stat. 272 (2001) (to be co [hereinafter "USA PATRIOT Act"].

significant threats to civil liberties, privacy and democratic traditions in U.S. history."[209] One effect of the Act is that it has made the approval process of wiretaps noticeably easier.[210] While only 1,003 warrants were approved in 2000 under the 1978 Foreign Intelligence Surveillance Act,[211] the USA PATRIOT Act allowed for the approval of 1,754 warrants in 2004.[212]

As previously discussed, the REAL ID Act of 2005 is another extensive piece of legislation which states that drivers licenses will only be accepted for "federal purposes"—like accessing planes, trains, national parks, and court houses—if they conform to certain uniform standards. U.S. passports are also subject to this legislation. Information contained in passports is highly sensitive and real dangers exist that this data could potentially be compromised through RFID contact-less transmission. Nevertheless, the technology has been incorporated into the new passport standards with little to no wide spread public outcry.

The lack of restrictive RFID legislation and the passage of federal proscriptive RFID legislation indicate that the public is not passionately opposed to RFID. Assuming that states pass legislation that reflects the views of their populace, the fact that only four RFID regulations bills have been passed in the years after RFID was first introduced shows that there is no rush to regulate the technology. This is further supported by the fact that only seventeen states have even addressed the issue in their state Congresses. Even those states that were finally able to pass and RFID bill did so only after numerous attempts.

Alternatively, other indicators seem to show that public support for invasive technologies is waning. For instance, immediately after the 9/11 attacks, a Harris Poll found that 68 percent of Americans supported a national ID system. By November of that year, a study conducted for the Washington Post found that only 44 percent of Americans supported national ID. A poll released in March 2002 by the Gartner Group found that 26 percent of Americans favored a national ID, and that 41 percent opposed the idea. Popular support for other surveillance technologies has declined as well.[213] Similarly, CNN, USA Today, and Gallup polled 1,003 adults for their opinions on the news that the National Security Agency has been conducting warrantless domestic surveillance, as well as opinions on the PATRIOT Act. Of those polled, 46 percent said that the warrantless surveillance was wrong and 38 percent polled said that the administration had gone too far in restricting civil liberties, up from the 28 percent result given in 2003, and the 11 percent result from 2002. On the PATRIOT Act, 74 percent of the public supported changing the law, with 50 percent wanting minor changes, 24 percent in favor of major

209. Electronic Frontier Foundation, *The USA Patriot Act*, http://w2.eff.org/patriot/.

210. USA PATRIOT Act §§ 201 & 202, 115 Stat. 272, 278.

211. Electronic Privacy Information Center, Foreign Intelligence Surveillance Act Orders 1979-2007, http://epic.org/privacy/wiretap/stats/fisa_stats.html.

212. *USA Patriot Act: Hearing Before the S. Select Comm. on Intelligence*, 109th Cong. 7 (2005) (testimony of Bob Barr, Former Member of Congress).

213. Electronic Privacy Information Center, Public Opinion on Privacy, http://epic.org/privacy/survey/.

changes and 7 percent calling for the law to be repealed.[214] Finally, in a telephone poll conducted on January 5-8, 2006 by the Washington Post and ABC News, 1,001 adults were asked, among other things, about their views on privacy rights and government surveillance measures. Sixty-four percent believed that federal agencies were intruding on Americans' privacy rights in investigating terrorism. Forty-six percent believed that those intrusions were not justified. Forty-four percent were worried that the Bush administration would go too far in compromising constitutional rights in order to investigate terrorism. Thirty-two percent placed a higher priority on the federal government respecting personal privacy than investigating possible terrorist threats, up 11 percent from 2003.[215]

Regardless, terrorism is still fresh on the minds of many Americans as terrorism-related articles continue to make front-page news and the issue remains a central component of the upcoming presidential election. Simply because Americans are less supportive of the Iraq War does not mean they have become complacent about terrorism. With attacks continuing since 9/11 in other locations such as the March 2003 train bombings in Madrid and the July 2005 London tube bombings as well as news of numerous thwarted terrorist attacks on American and foreign soil, Americans' attitudes toward relinquishing a certain degree of privacy of the sake of security is likely to continue.

3. A New Era in Privacy Regulation?

Some experts argue that a significant shift in U.S. privacy policy will not occur until some crisis or highly publicized event forces us to look at the issue from a new perspective.[216] Just as the events of 9/11 changed the way American view privacy concerns, another equally as dramatic event may be necessary to swing the pendulum the other way. At the same time, the public opinion polls suggest that in at least some respects, American attitudes toward privacy are returning to their pre-9/11 status.

VI. CONCLUSION

Like all new technologies, RFID promises exciting prospects for the way we conduct our everyday lives. At the same time, it important to be vigilant of the potential privacy concerns posed by the technology. Any wireless technology that freely passes highly sensitive personal information through the air should be scrutinized to ensure that adequate safety precautions exist. As discussed in this Note, the legal framework for regulating RFID may already be in place, thus warranting no further action by Congress. Moreover, the limitations of

---

214. *Poll Finds U.S. Split over Eavesdropping*, CNN, Jan. 10, 2006, http://edition.cnn.com/2006/POLITICS/01/10/poll.wiretaps/.

215. Dan Balz & Claudia Deane, *Differing Views on Terrorism*, WASHINGTON POST, Jan. 11, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/01/10/AR2006011001192. html.

216. Valetk, *supra* note 128, at n.189 (citing James. P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. LAW. REV. 1, 83 (2003)).

these devises may require additional protections or the inherent limitations of the technology such as the short read range of RFID tags and the inability for unauthorized third-party interception may prevent any real threat to individual privacy.

The goal of this Note is not to come to a conclusive answer as to whether or not lawmakers should enact legislation restricting the use of RFID. Instead, it has analyzed the various social and political factors that might lead to states adopting, or failing to adopt, RFID restrictive or prescriptive legislation. This article may also serve as a policy guide for lawmakers. In light of the various benefits of RFID including the ease, convenience, and security provided by the technology as well as the fact that some level regulatory laws already seem to be in place, it is unlikely that states will pass any significant RFID legislation in the future beyond what has already been enacted. This is particularly true considering the greater affinity that Americans have expressed toward government since 9/11. With these conclusions in mind, opponents of RFID must achieve two important objectives: (1) provide consumers with a clear understanding of what RFID is, how it works, and its potential ramifications and (2) convince them that RFID privacy concerns outweigh any economic benefits, greater convenience, or added security. The public's view could also change if some striking problem with RFID arises but for the time being, there seems little to stop RFID as we willingly, perhaps unknowingly, ride the wave of its silent revolution.