

A CALL TO ACTION: THE FOURTH AMENDMENT, THE FUTURE OF RADIO FREQUENCY IDENTIFICATION, AND SOCIETY

*David J. Warner**

I. INTRODUCTION

Imagine a world where children all wear wristbands about the size of a Zippo lighter¹—not as the newest fashion statement, but instead for security. These wristbands can transmit a signal with an effective range of over two football fields, narrowing down each child's position to within thirty feet. Furthermore, the system can track the children over a two square mile area surrounding their school. If a child walks off their path or does not make it to school on time, the centralized system automatically sends an e-mail or text message to the child's parents. Or, if the child is in trouble, they can press a warning button on the wristband, and a call is routed to local authorities. In addition, cars near the children's school are fitted with the same technology, and if a vehicle drives near a child, a voice prompt will alert the driver (giving a separate warning if the child has pressed their warning button).

While this scenario may seem fitting for the newest science fiction motion picture, the scene is reality in Yokohama City, Japan.² In a joint test program between an American maker of radio frequency identification ("RFID") tags and a Japanese automaker,³ a

* J.D. Candidate, May 2008, Loyola Law School, Los Angeles; B.A., Political Science and History, May 2003, University of Minnesota. I would like to thank Professor John T. Nockleby, Aaron M. Fennimore, Emma S. D'Onofrio, and Tina M. Carstens for their guidance and suggestions throughout the writing process.

1. 2.5 inches by 1.5 inches by 0.5 inches

2. Claire Swedberg, *RFID Watches Over School Kids in Japan*, *RFID JOURNAL*, Dec. 16, 2005, <http://www.rfidjournal.com/article/articleview/2050/1/1>.

3. *Id.*

new era of RFID technology is becoming reality. The greatest question from this scenario is where does the technology go from here?

The theory behind RFID technology dates back to the study of electromagnetic waves in the 19th century.⁴ However, the first practical step towards RFID technology was in World War II, fueled by Britain's desire to not shoot down their own aircraft.⁵ The Identification, Friend or Foe system allowed the Allies to carry transponders in their aircraft, allowing air controllers to distinguish ally from enemy.⁶

Over the years,⁷ this technology has advanced in a myriad of directions—from an alternative to the Universal Product Code (“UPC”) on consumer products,⁸ to a convenient way to pay highway tolls.⁹ In the coming years, RFID technology is poised for further advancements, as processors, batteries, and transponders are decreasing in cost and size while increasing in power.¹⁰ Although these future uses may be within reach, several questions remain. What legal boundaries are implicated by future RFID uses? Even if a technology is “legal,” is our society prepared to understand and

4. DAVID C. WYLD, IBM CTR. FOR THE BUS. OF GOV'T, RFID: THE RIGHT FREQUENCY FOR GOVERNMENT 9 (2005), available at <http://www.businessofgovernment.org/pdfs/WyldReport4.pdf>. Among the pioneers were Michael Faraday, Frederick Hertz, and Guglielmo Marconi. *Id.* In fact, Hertz specifically studied using radio frequencies to reflect waves from objects—a precursor to RFID technology. *Id.*

5. See The British Invention of Radar, http://www.vectorsite.net/ttwiz_01.html (last visited Feb. 8, 2007).

6. JEREMY LANDT, ASS'N FOR AUTOMATIC IDENTIFICATION & DATA CAPTURE TECHS., SHROUDS OF TIME: THE HISTORY OF RFID 3–4 (2001), http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf.

7. Charles Walton (no relation to the founder of Wal-Mart, the corporation that leads the way in promoting RFID technology for consumer goods) is considered the author of the first fundamental patent of RFID technology—a “radio-operated door lock” in 1973. See WYLD, *supra* note 4, at 10; see also U.S. Patent No. 3,816,708 (filed May 25, 1973). Walton originally pitched his idea of a keyless lock to General Motors but was dismissed because the idea was “too Buck Rogers.” WYLD, *supra* note 4, at 10. Instead, Walton sold his idea to the lock maker Schlage, who then created the first smart card—allowing doors to be opened by waving a card in front of a reader. *Id.*

8. See WYLD, *supra* note 4, at 19.

9. See E-ZPass Interagency Group, <http://www.e-zpassag.com> (last visited Feb. 8, 2007); FasTrak, <http://www.bayareafastrak.org> (last visited Feb. 8, 2007).

10. See Sanjay E. Sarma et al., *Radio-Frequency Identification: Security Risks and Challenges*, CRYPTOBYTES, Spring 2003, at 3–4, available at http://www.rsasecurity.com/rsalabs/cryptobytes/CryptoBytes_March_2003_lowres.pdf (discussing the growth potential for RFID created by reducing the cost of RFID tags below \$0.10).

face these new technologies? And what steps can our society take to properly embrace (or reject) emerging RFID technological uses?

In Part II, this Note discusses RFID technology and a few of its many current uses. Next, in Part III, the applicable legal standards and precedents under the Fourth Amendment are discussed and then analyzed in light of the current RFID technology. Then, in Part IV, this Note looks at possible future uses of RFID technology and analyzes these future uses in light of their legal implications. Lastly, in Part V, the Note concludes that only through a three-prong approach can RFID technology be properly implemented into society: adequate legislative oversight, proper private/public sector restraint, and greater consumer understanding.

II. RADIO FREQUENCY IDENTIFICATION (RFID)

A. *What exactly is RFID technology?*

In order to better apply Fourth Amendment jurisprudence to RFID technology, the workings and uses of RFID must first be explained. RFID belongs to the larger family of automatic identification, which includes smart cards, bar code systems, and biometric systems.¹¹ Unlike some of its cousins, RFID uses radio waves to transmit information without requiring contact or line of sight.¹² The three main components of an RFID system are the tag, reader, and software used to process this information.¹³

The tag is a combination of a small microchip, an antenna, and a casing to hold the components together.¹⁴ These tags are divided into two main categories: passive and active. With a passive RFID tag, the transmission works like the game “Marco Polo.”¹⁵ The reader (usually in a fixed location, e.g., near a door) will say “Marco” in the form of a radio wave at a designated frequency.¹⁶ The chip inside the RFID tag then takes that radio energy and echoes back its answer,

11. WYLD, *supra* note 4, at 9. In addition, RFID can be included with radar and GPS as systems that use radio frequency to determine a given object’s location.

12. *Id.* at 12.

13. *Id.* at 16.

14. *Id.*

15. Ryan Singel, *American Passports to Get Chipped*, WIRE, Oct. 21, 2004, <http://www.wired.com/news/privacy/0,1848,65412,00.html>.

16. *Id.*

but instead of simply saying “Polo,” the chip will reply with its programmed response.¹⁷ With an active RFID tag, the tag has its own power source and can actively transmit—in essence, allowing the tag to regularly say “Polo” without the reader needing to say “Marco” first.¹⁸

B. Current Uses

RFID technology currently has many uses in commercial, personal, and governmental settings. While Senator Patrick Leahy has described RFID tags as “barcodes on steroids,”¹⁹ RFID has many more uses than simply replacing the UPC bar code found on all commercial products.²⁰

In commercial settings, RFID is already seeing global use in smart cards, allowing access into buildings without the use of keys or magnetic swipe cards.²¹ In addition, libraries are coding all books with RFID tags, allowing librarians to track books and find misplaced items without manually looking on every shelf.²² Moreover, golfers can now track down an errant drive using a hand-held RFID reader to find their RFID-imbedded golf ball.²³ Other

17. *Id.*

18. In fact, one of these active RFID tags, the AeroScout T2, has the ability to transmit “Polo” 8 times per second at a range of 600 feet (outdoors) and could go on doing so for three years on one replaceable AA battery. AeroScout T2 Data Sheet, <http://www.aeroscout.com/data/uploads/AeroScout%20T2%20Tag%20Data%20Sheet.pdf> (last visited Feb. 8, 2007).

19. Russell Fox & Laura Newman Rychak, *The Potential Challenges of RFID Technology*, ADVISORY (Mintz Levin Cohen Ferris Glovsky & Popeo PC, Boston, Mass.), May 2004, at 1, available at <http://www.mintz.com/images/dyn/publications/CommunicationsAdvisory.0504.pdf> (quoting Senator Patrick Leahy, The Dawn of Micro Monitoring: Its Promise, and its Challenges to Privacy and Security, Remarks at Conference on Video Surveillance: Legal and Technological Challenges, Georgetown University Law Center (Mar. 23, 2004), <http://www.law.georgetown.edu/webcast/eventDetail.cfm?eventID=33>).

20. For a discussion of UPC versus the RFID version, using the Electronic Product Code (“EPC”), see WYLD, *supra* note 4, at 19. With the traditional UPC code, suppliers were limited to identifying “only” 100,000 products for 100,000 manufacturers. *Id.* Now, with the EPC, each item can have its own unique identifier—up to thirty-three trillion total products; a number greater than the total number of atoms in the entire universe. *Id.*

21. *See id.* at 65.

22. *Id.* at 7.

23. Mark LaPedus, *Radar Golf Claims Breakthrough with RFID Golf Balls*, INFORMATION WEEK, Jan. 25, 2005, <http://www.informationweek.com/story/showArticle.jhtml?articleID=57703713>. Interestingly, the maker of these golf balls, Radar Golf, Inc., claims that their balls (approved by the United States Golf Association) perform as well, if not better, than standard golf balls made by Titleist, Callaway, Nike, and Maxfli. *Id.* Their system sells for \$249, which includes one dozen golf balls and a hand-held reader that has an effective range of 100 feet. *Id.*

commercial uses include tagging hospital equipment (to locate quickly during an emergency and reduce theft), all livestock in the United States (in case of another Mad Cow disease outbreak), and prescription drug containers (so that pharmacists can quickly recognize a counterfeit drug).²⁴

As far as personal uses, VeriChip Corporation developed in 2001 an implantable RFID tag that is inserted under the skin.²⁵ So far, two groups have enthusiastically endorsed this procedure. The first are club-goers in Barcelona, who prefer the RFID tag to carrying their identification and credit cards.²⁶ The second are Mexican government officials, who use the implanted RFID tags to access restricted places and as an anti-kidnapping measure.²⁷

In addition, as mentioned in Part I, schoolchildren in Japan are being tagged with active RFID tags on their wrists.²⁸ These tags send a signal once per second to special readers, which can then relay the information using Yokohama City's existing wireless network.²⁹

Lastly, in terms of government uses, electronic passports have received the most attention.³⁰ These passports have an RFID tag imbedded in the passport itself and are being used by the United

24. WYLD, *supra* note 4, at 8.

25. VeriChip Corporation, http://www.verichipcorp.com/content/company/our_technology (last visited Feb. 8, 2007).

26. Simon Morton, *Barcelona Clubbers Get Chipped*, BBC NEWS, Sept. 29, 2004, <http://news.bbc.co.uk/2/hi/technology/3697940.stm>. The owner of the club (the first to be implanted) envisions the system as the ultimate VIP membership. *Id.* The doorman will scan the club-goers when they enter the club, and their personal identification number will connect with a database of the patron's preferences (e.g., drinks, music, seating). *Id.* By the time the patron makes it to the bar, their favorite drink will be waiting for them, and the cost of the drink will have been debited from their account. *Id.*; see also Baja Beach Club, <http://www.bajabeach.es> (last visited Feb. 8, 2007).

27. Interview by Elizabeth Juarez with Marco Huitron, Official, Mexican Att'y Gen.'s Office (Katherine Albrecht trans., Oct. 22, 2004), available at <http://www.spsychips.com/press-releases/mexican-translation.html> (last visited Feb. 8, 2007). It should be noted that in addition to these two diverse groups, VeriChip's implantable RFID tag has been used in natural disasters, such as Hurricane Katrina, to tag the bodies of victims among debris and rubble for later removal and identification. VeriChip Corporation, Emergency Management, http://www.verichipcorp.com/contents/solutions/emergency_management (last visited Feb. 8, 2007).

28. Swedberg, *supra* note 2.

29. *Id.* The AeroScout T2 active tags being used comply with the 802.11 wireless internet standard and transmit on the 2.4 GHz range for maximum distance and power. *Id.*

30. For a discussion of the potential privacy and security issues with RFID-imbedded passports, see ARI JUELS ET AL., SECURITY AND PRIVACY ISSUES IN E-PASSPORTS (2005), <http://eprint.iacr.org/2005/095.pdf>. For a video of security concerns relating to electronic passports, see RFID Passport Shield Failure Demo—Flexilis, <http://www.youtube.com/watch?v=-XXAqraF7pI> (last visited Feb. 8, 2007).

States and twenty-four other countries whose citizens can enter the United States under the Visa Waiver Program.³¹ Beyond electronic passports, the United States Government Accountability Office (“GAO”) released a report in May 2005 identifying sixteen government departments and agencies that have over twenty-five current uses for RFID technology, ranging from the Department of Energy’s tracking nuclear material to the Social Security Administration’s warehouse management system.³² In addition, an airport in Hungary is using RFID tags to track all passengers in the airport from the moment they enter the airport until they board the plane.³³

III. FOURTH AMENDMENT JURISPRUDENCE

Although a case questioning the constitutionality of current uses of RFID technology has not come before the U.S. Supreme Court,³⁴ previous court cases can provide a framework of protections provided. The Fourth Amendment states,

31. See Press Release, U.S. Dep’t of State, Most Visa Waiver Program Nations Meet Electronic Passport Deadline (Oct. 27, 2006), available at <http://usinfo.state.gov/xarchives/display.html?p=washfile-english&y=2006&m=October&x=200610271436211CJsamohT0.1565821>. For information on the developments of the United States using electronic passports, see The U.S. Electronic Passport, http://travel.state.gov/passport/eppt/eppt_2498.html (last visited Feb. 8, 2007).

32. U.S. GOV’T ACCOUNTABILITY OFFICE, NO. 05-551, INFORMATION SECURITY: RADIO FREQUENCY IDENTIFICATION TECHNOLOGY IN THE FEDERAL GOVERNMENT 13 (2005), available at <http://www.gao.gov/new.items/d05551.pdf>. This report was most noteworthy for the conclusion of the GAO—that although the government has been enthusiastic in implementing RFID technology, the agencies were largely unaware of the legal/privacy implications of their actions. *Id.* at 18. Of the sixteen agencies surveyed, only one responded that there may be some legal issues—the other fifteen said there would be no legal issues surrounding the use of RFID technology. *Id.* at 17–18.

33. Gemma Simpson, *New RFID Tech Would Track Airport Passengers*, CNET NEWS, Oct. 13, 2006, http://news.com.com/New+RFID+tech+would+track+airport+passengers/2100-7355_3-6125799.html. For an informative view of what an RFID-enabled airport of the future may look like, see RFID: Airport Tracking, <http://www.spychips.com/RFIDairport.html> (last visited Feb. 8, 2007). Compex, Inc., who has been in negotiations with the Transportation and Security Administration (“TSA”) to implement their comprehensive system, produced this video and patented the process in 2005. See CompEx, Inc., <http://www.compexinc.com> (last visited Feb. 8, 2007); U.S. Patent No. 6,970,088 (filed Oct. 17, 2003) (issued Nov. 29, 2005).

34. For an entertaining mention of RFID technology (and the only case to mention RFID in a privacy context), see *Montana v. 1993 Chevrolet Pickup*, 116 P.3d 800, 806 (Mont. 2005) (Nelson, J., concurring) (“Like it or not, I live in a society that accepts . . . radio frequency identification devices already implanted in the family dog and soon to be integrated into my groceries, my credit cards, my cash and my new underwear.”).

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.³⁵

The “well-known historical 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.”³⁶ However, “the Fourth Amendment cannot be translated into a general constitutional ‘right to privacy.’”³⁷ Underneath these principles is a two-prong approach to Fourth Amendment jurisprudence: (1) whether the action taken was a “search”; and (2) if such action was a search, whether the search was unreasonable.³⁸

A. *Early Case Law: Tort, Then Reasonable Expectations*

In *Olmstead v. United States*,³⁹ the government used a wiretapping device to listen to defendant’s telephone conversations without trespassing on the property of the defendant.⁴⁰ The Court found that the actions did not constitute a search under the Fourth Amendment.⁴¹ The Court concluded that “[t]he language of the Amendment can not be extended and expanded to include telephone wires reaching to the whole world from the defendant’s house or office.”⁴² In reaching this decision, the Court focused on the tort of trespass,⁴³ concluding that because the government did not physically

35. U.S. CONST. amend. IV.

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

37. *Katz v. United States*, 389 U.S. 347, 350 (1967); *see also id.* at 350 n.5 (discussing other amendments that protect privacy: First, “freedom to associate and privacy in one’s associations”; Third, no quartering of soldiers; and Fifth, the right to a “private enclave where he may lead a private life”). Later, in *Griswold v. Connecticut*, the Court also found “zones of privacy” in the penumbras and emanations of the Ninth Amendment. 381 U.S. 479, 484 (1965).

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

39. 277 U.S. 438 (1928).

40. *Id.* at 456–57.

41. *Id.* at 464.

42. *Id.* at 465.

43. *See* RESTATEMENT (SECOND) OF TORTS § 158(a) (1977) (“One is subject to liability to another for trespass . . . if he intentionally enters land in the possession of the other . . .”).

enter onto the defendant's land, there was no trespass and thus no "search."⁴⁴

Over the next forty years, the Court attempted to continue applying the standard of *Olmstead* with varying success. In *Katz v. United States*,⁴⁵ the Court again faced an intercepted telephone conversation—this time, involving a telephone booth.⁴⁶ The government in this case had attached a listening device to the outside of the telephone booth; thus, they did not physically enter the telephone booth.⁴⁷ However, the Court concluded that the trespass rule of *Olmstead* was no longer valid law.⁴⁸ Instead, the Court focused on whether the defendant sought to keep the conversation private.⁴⁹ In his concurrence, Justice Harlan delivered the oft-quoted rule: "[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"⁵⁰

*B. New Technology #1 (Radio Transmitters):
Visual Augmentation or Search?*

In the early 1980s, the Court faced a new technology that threatened Fourth Amendment protections: radio transmitters. In *United States v. Knotts*,⁵¹ the police placed a radio transmitter in a container of chloroform that was purchased by the defendant.⁵² The police then followed the transmitter (using a video reader) from Minnesota to a remote lake in Wisconsin.⁵³ Police used the evidence

44. *Olmstead*, 277 U.S. at 464 ("There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants."). *But see id.* at 472 (Brandeis, J., dissenting) (discussing how the Fourth Amendment and federal legislation could evolve to find that the new technology of wiretapping would be an unreasonable search).

45. 389 U.S. 347 (1967).

46. *Id.* at 348.

47. *Id.*

48. *Id.* at 353.

49. *Id.* at 351–52 (noting that "what [defendant] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected"). Conversely, the Court also stated that what a person "knowingly exposes" to the public, even in one's own home, is not constitutionally protected. *Id.* at 351.

50. *Id.* at 361 (Harlan, J., concurring).

51. 460 U.S. 276 (1983).

52. *Id.* at 278.

53. *Id.* at 278–79.

along with video surveillance to obtain a warrant, seizing drugs inside the lake cabin.⁵⁴ The Court held that the use of the radio transmitter was constitutional and did not amount to a “search” under the Fourth Amendment.⁵⁵ The Court specifically stated, “Nothing in the Fourth Amendment prohibited the police from *augmenting* the sensory facilities bestowed upon them at birth with such enhancement as science and technology afforded them in this case.”⁵⁶ Meaning, a car *could* have followed the defendant, but the police simply chose more efficient means.

In *Knotts*, the Court made two statements that would foreshadow its future cases. First, the Court noted that the radio transmitter was not used to discover any information from inside the cabin or that was not visible to the naked eye.⁵⁷ Second, after the defendant argued that using a radio transmitter amounts to “twenty-four hour surveillance of any citizen of this country,” the Court concluded that “if such dragnet type law enforcement practices” should ever occur, then the Court would revisit the issue and determine whether a different rule should apply.⁵⁸

In *United States v. Karo*,⁵⁹ the Court faced the first of those two questions: what if the technology *does* allow the police to see what could otherwise not be seen by the naked eye? In *Karo*, Drug Enforcement Agency (“DEA”) agents placed a radio transmitter in a five-gallon drum of ether (as part of a larger shipment) that defendant bought and then transported from one location to another, in an attempt to outmaneuver authorities.⁶⁰ At different points in the surveillance, the DEA agents used solely the information from the radio transmitter (and not their naked eye) to conclude that the drums of ether were still at the location.⁶¹ The Court concluded that a warrantless search is unreasonable where the government uses an electronic device to reveal information otherwise not obtainable from

54. *Id.* at 279.

55. *Id.* at 285.

56. *Id.* at 282 (emphasis added).

57. *Id.* at 285.

58. *Id.* at 283–84.

59. 468 U.S. 705 (1984).

60. *Id.* at 708–10, 714.

61. *Id.* at 715.

outside the home.⁶² Thus, the question from *Knotts* was answered: if the tracking technology allows the authorities to “see” inside the home in a way impossible with their naked eye, then it is a search, and, absent an exception, a warrant is required to make the search reasonable.

*C. New Technology #2 (Thermal Imager):
How much Augmenting is Too Much?*

In *Kyllo v. United States*,⁶³ the Court faced another new technology and its effect on the Fourth Amendment: a thermal imager.⁶⁴ A Department of Interior official suspected that the defendant was growing marijuana in his home.⁶⁵ The official borrowed an off-the-shelf thermal imager to use on the defendant’s home, believing the imager would show heat from the lamps necessary to grow marijuana.⁶⁶ Sitting in the official’s car, the handheld imager showed an unusual heat source radiating from the defendant’s garage.⁶⁷ Along with tips from informants and the defendant’s energy bills, the thermal images were enough to secure a warrant.⁶⁸ Using the warrant, the police then entered the defendant’s home and found marijuana plants.⁶⁹ The Ninth Circuit Court of Appeals found that the action of the authorities was not a search under the Fourth Amendment because the imager “did not expose any intimate details of Kyllo’s life,” just “amorphous ‘hot spots’ on the roof and exterior wall.”⁷⁰

The U.S. Supreme Court reversed the Ninth Circuit, in part by looking past the simple technology used in *Kyllo* to the advanced technologies of the future.⁷¹ In addition, the Court reaffirmed the

62. *Id.* at 716.

63. 533 U.S. 27 (2001).

64. *Id.* at 29. A thermal imager detects infrared energy, which is emitted from all objects based on their temperature and is displayed on the camera as warm and cool colors relative to objects nearby. FLIR Systems, <http://www.flirthermography.com/about> (last visited Feb. 8, 2007).

65. *Kyllo*, 533 U.S. at 29.

66. *Id.*

67. *Id.* at 30.

68. *Id.*

69. *Id.*

70. *United States v. Kyllo*, 190 F.3d 1041, 1047 (9th Cir. 1999).

71. *Kyllo*, 533 U.S. at 36.

principles of *Karo*, with an added twist: “We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical ‘intrusion into a constitutionally protected area’ constitutes a search—at least where (as here) the technology in question is not in general public use.”⁷² In his dissent, Justice Stevens focused on these last few words (the departure from the *Karo* decision) about “general public use,” stating that “this criterion is somewhat perverse because it seems likely that the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available.”⁷³

*D. New Technology #3 (RFID Technology):
A “More Sophisticated System” or Merely Augmenting?*

In light of the Court’s Fourth Amendment jurisprudence, certain principles can be distilled.

First, as previously mentioned,⁷⁴ “a ‘search’ occurs when an expectation of privacy that society is prepared to consider reasonable is infringed.”⁷⁵ However, when a person is moving in public (e.g., riding in a car), they have “no reasonable expectation of privacy in [their] movements from one place to another.”⁷⁶ Thus, the Court most likely will not consider any tracking using RFID while traveling in public a “search” under the Fourth Amendment. However, once the RFID tag enters the home and is removed from public view, the Fourth Amendment would protect any tracking or information gathered.

Second, the Court has not applied or tested the statement in *Kyllo* of technology “not in general public use.”⁷⁷ The majority was

72. *Id.* at 34 (citations omitted).

73. *Id.* at 47 (Stevens, J., dissenting).

74. *See supra* text accompanying note 50.

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

76. *United States v. Knotts*, 460 U.S. 276, 281 (1983). *Contra* April A. Ottenberg, Note, *GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court’s Theory of the Public Space Under the Fourth Amendment*, 46 B.C. L. REV. 661, 693–94 (2005) (discussing how in light of new technologies, for example, GPS (and by inference RFID), the Court should reconsider its policy regarding public space and the definition of “search”).

77. While no case has interpreted the “general public use” requirement from *Kyllo*, there has been much speculation about what effect this standard will have on Fourth Amendment jurisprudence and privacy in general. *See, e.g.*, Derek T. Conom, Comment, *Sense-Enhancing Technology and the Search in the Wake of Kyllo v. United States: Will Prevalence Kill Privacy?*, 41 WILLAMETTE L. REV. 749, 763–65 (2005) (discussing two alternatives to the “general public use” language: ignore it or scrutinize it); Casey Holland, Note, *Neither Big Brother Nor Dead*

arguing that, for example, as RFID readers become more prevalent in society, individuals will have a better understanding of their capabilities and will act accordingly to keep private matters outside the public realm.⁷⁸ However, Justice Stevens' criticism of this statement would seem to hold true for RFID technology (that as a technology comes into general public use, the need for protection is greater).⁷⁹ Individuals will never be able to fully protect themselves from a new technology, no matter the amount of notice and disclosure.

The majority's formulation would seem to lead to escalation by both sides—consumer and private enterprise/government. Using the facts of *Kyllo*, if thermal imagers were of general public use (however that is defined), the defendant could have wrapped his entire house in extra insulation, in an effort to keep the heat from registering. However, if such a practice becomes widespread, companies will merely develop a better thermal imager that is able to register smaller differences in amounts of heat. The same is true with RFID technology. It is possible to block the transmission of the RFID tag using a Faraday cage,⁸⁰ but if such actions become commonplace, companies will simply build technologies that overcome this obstacle.⁸¹

Third, in *United States v. Jacobsen*,⁸² the Court concluded that the Fourth Amendment applies only to government action—not to action by a private individual, no matter how unreasonable.⁸³ The

Brother: The Need for a New Fourth Amendment Standard Applying to Emerging Technologies, 94 KY. L.J. 393, 414 (2005) (suggesting a three-stage approach to “general public use”: (1) when new, use *Kyllo*; (2) once “relatively common” in the public, use *Katz*'s “reasonable expectation of privacy”; and (3) when in frequent use by the public, a reasonable expectation is per se unreasonable and *Katz* doesn't apply).

78. See *Kyllo*, 533 U.S. at 34.

79. See *id.* at 47 (Stevens, J., dissenting).

80. While having an impressive sounding name, a Faraday cage can be as simple as wrapping the RFID tag in tin foil or as complex as blocking electromagnetic waves from entering/exiting many United States government buildings. For example, the DIFRwearR RFID Blocking Wallet places a layer of metal in the lining of a leather wallet to create a Faraday cage. ThinkGeek, RFID Blocking Wallet, <http://www.thinkgeek.com/gadgets/security/8cdd/> (last visited Feb. 8, 2007).

81. In fact, Rohm and Haas, a materials company, has developed a powder coating that can, at times, overcome the effects of a Faraday cage. See Rohm and Haas Powder Coatings, Faraday Cage Penetration, http://www.rohmhaas.com/powdercoatings/tech/application_answers/app_ans_faraday.html (last visited Feb. 8, 2007).

82. 466 U.S. 109 (1984).

83. *Id.* at 113.

two caveats on this statement are that the Fourth Amendment applies if a private individual is acting as an agent of the government or with the participation or knowledge of the government.⁸⁴

Thus, for example, Wal-Mart could sell products with RFID tags (e.g., EPC)⁸⁵ and not disable the tags at the point of sale.⁸⁶ Wal-Mart could then (theoretically, of course) follow customers home and use an RFID reader (from outside the house) to read whether these products are in their home (and what other products are in their home and where they bought them). If a government official were to conduct this activity, it would run afoul of the Fourth Amendment. However, since Wal-Mart is a private entity, the customer would have no Fourth Amendment redress.⁸⁷

Lastly, “when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information.”⁸⁸ An example of this is a “pen register.”⁸⁹ In *Smith v. Maryland*,⁹⁰ the Court held that requesting a pen register was not a search under the Fourth Amendment and thus did not require a warrant.⁹¹ Congress then passed the Electronic Communications Privacy Act of 1986 (“ECPA”), which created a statutory requirement of obtaining a warrant before requesting a pen register,⁹²

84. *Id.*

85. See WYLD, *supra* note 4, at 19 (discussing the EPC versus the current UPC standard); see also *supra* note 20.

86. Disabling, or “killing,” an RFID tag involves using an electromagnetic pulse to destroy the circuits of the chip. Jonathan Collins, *RFID-Zapper Shoots to Kill*, RFID JOURNAL, Jan. 23, 2006, <http://www.rfidjournal.com/article/articleview/2098/1/1/>. Two Germans developed a system to kill RFID tags using a disposable camera and a coil of wire. *Id.*

87. On the other hand, the customer may have a tort claim against Wal-Mart in this hypothetical. See RESTATEMENT (SECOND) OF TORTS § 652B (1977) (“One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another . . . is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.”).

88. *United States v. Jacobsen*, 466 U.S. 109, 117 (1984).

89. A “pen register” is a system which records the dialing habits of any telephone or electronic device. See 18 U.S.C. § 3127(3) (2000).

90. 442 U.S. 735 (1979).

91. *Id.* at 744 (noting that by dialing telephone numbers, the defendant “voluntarily conveyed numerical information to the telephone company” and “assumed the risk that the company would reveal to police the numbers”).

92. 18 U.S.C. § 3121(a) (2000). However, evidence obtained in violation of the ECPA can still be admitted in a criminal trial, because the ECPA does not specifically state that such

effectively overriding the Court's decision.⁹³ However, in areas where Congress has not acted (e.g., RFID technology), the principle of "assumption of risk" with third-party companies still governs.

IV. FUTURE USES OF RFID TECHNOLOGY

A. An RFID-Enabled Future

Now that *current* RFID uses have been discussed in light of the Fourth Amendment, this Article will take the legal discussion a step further: *future* uses of RFID. To illustrate some of the potential uses for RFID technology in the future, this author will follow a fictitious person, Jane Doe, through her Saturday morning in the near future.⁹⁴

Jane wakes up to the sound of her personal alarm clock and walks over to the medicine cabinet. The "Online Medicine Cabinet" recognizes her face and recommends that she take her morning prescription.⁹⁵ The cabinet senses (based on a weight difference) that Jane has taken her morning pill and wishes her a good day as she walks down to the kitchen.⁹⁶

In the kitchen, the automated household assistant tells Jane that a recall has been ordered on the blender she bought last week and also that her television's warranty has expired.⁹⁷ Jane is puzzled by how the house knew she bought that blender last week, but then she

evidence must be excluded. *See* United States v. Thompson, 936 F.2d 1249, 1251–52 (11th Cir. 1991). For further discussion on legislative oversight and the role that the ECPA could play with regard to RFID regulation, see *infra* Part V.A.

93. While *Smith v. Maryland* and the Electronic Communications Privacy Act of 1986 affect the status of federal law, individual states are free to interpret their own constitutions. In *People v. Blair*, 602 P.2d 738 (Cal. 1979), the California Supreme Court held that under Section 13 of Article I of the California Constitution, officers would need a warrant to access information in a pen register. *Id.* at 746. However, Proposition 8, codified in Section 28(d) of Article I of the California Constitution, superceded this decision. As interpreted in *People v. Lance W.*, 694 P.2d 744 (Cal. 1985), pen registers can no longer be excluded from entering into evidence, as long as the information is relevant, because pen registers are only protected under the California Constitution, not the Fourth Amendment. *Id.* at 753.

94. As noted by the citations throughout this section, all technologies mentioned have either been developed and patented or patents have been applied for, but not yet received.

95. U.S. Patent No. 6,539,281 (filed Apr. 23, 2001) (issued Mar. 25, 2003).

96. *See* Accenture, Online Medicine Cabinet, http://www.accenture.com/Global/Services/Accenture_Technology_Labs/R_and_I/OnlineMedicineCabinet.htm (last visited Feb. 8, 2007).

97. IBM has developed an internet-enabled "household system for tracking and managing RFID" items. U.S. Patent No. 7,118,037 (filed Sept. 16, 2004) (issued Oct. 10, 2006). This system will automatically track all RFID-enabled items in the house via an online database and link these items to useful information, e.g., warranties and product recalls.

remembers that all of her purchases have little tags on them that can “talk” to her house. Jane grabs a breakfast burrito from the refrigerator and places it in the microwave. The microwave automatically knows that a breakfast burrito has been placed in it, finds the proper cooking time and temperature from the Internet, and begins working.⁹⁸ Jane wonders what life was like back when people had to figure out on their own the amount of time and at what temperature to cook items in a microwave.⁹⁹

Next, Jane gets into her new car and drives to the grocery store. The trip is seven miles on the interstate, and Jane is happy that she is able to make the seven-mile trip in under six minutes. However, she will not be happy in one week when she receives an automatic speeding ticket in the mail for driving an average of 70 miles per hour in a 65 miles per hour zone.¹⁰⁰

Jane arrives at the automated parking structure, which informs her via a video screen that there are five available spots on level three.¹⁰¹ She parks in the first spot and walks towards the entrance to the supermarket.

As she is walking in, a man passes by coming close to but not actually touching, Jane. Little does Jane know that this man just scanned every RFID item Jane has by using his personal digital assistant (“PDA”) device.¹⁰² This includes the RFID chips in her

98. See U.S. Patent No. 7,133,739 (filed May 2, 2003) (issued Nov. 7, 2006).

99. According to the inventors of the “intelligent microwave oven,” in the past, when users set their own cooking time and temperature, “[d]inners may be ruined or homes burned down because of a user erroneously setting the wrong cooking time or temperature.” *Id.*

100. The same company that is producing the airport tracking system (CompEx, Inc.) has also developed a traffic monitoring system called “TrafficLinx.” CompEx, Inc., http://www.compexinc.com/?_core_cnt_SetActiveGroup=153 (last visited Feb. 8, 2007). In the most practical of scenarios, RFID readers would be placed at all entrance and exit ramps for major roadways. *Id.* These readers would scan the RFID tags embedded in license plates as vehicles drive by. *Id.* This data could then be processed in a central database, cross-referencing with any stolen vehicles or Amber alerts. *Id.* In addition, readers would also be placed inside police squad cars, allowing police to actively scan all vehicles near them on the road. *Id.*

101. See U.S. Patent No. 7,135,991 (filed Mar. 10, 2006) (issued Nov. 14, 2006). Developed by BellSouth, the system includes the ability to take vehicle information and compare it to personal information about the owner. *Id.* For example, if the owner cannot find their vehicle, they can approach a kiosk, where they enter information about themselves, and the system tells the owner where their vehicle is. *Id.*

102. Skimming (i.e., stealing) RFID signals can be as easy as a coil of wire and a “cloner” device. See Annalee Newitz, *The RFID Hacking Underground*, WIRED, May 2006, http://www.wired.com/wired/archive/14.05/rfid_pr.html. Accenture has also developed a system called the “Real-World Showroom,” which allows “shoppers” to use a PDA or laptop computer to scan what other people are wearing and then enabling them to purchase these items online. See

clothes, wallet, cellular phone, and car keys. The man then uses a computer program to extract the car's RFID code and uses his own PDA to emulate the RFID tag in Jane's car keys.¹⁰³ The man then drives away with the vehicle, using the nearest interstate freeway.

Unaware that her vehicle is gone, Jane enters the supermarket and is immediately greeted by an automated voice, "Good morning, Ms. Doe." Jane looks around and sees the digital assistant—a video screen that can interact with customers and "knows" Jane based on the RFID-embedded loyalty card in Jane's wallet.¹⁰⁴ If Jane were a highly valued customer, a manager may be alerted and sent over to assist Jane.¹⁰⁵ The video asks, "Would you like your shopping list for today?" Jane replies, "Yes. Where are tortillas located?" The digital assistant informs her that tortillas are in aisle seven, halfway down the left-hand side. The voice then offers to send these directions via a text message to Jane's phone.

As Jane walks down the aisles, the RFID tag/reader systems track her every move.¹⁰⁶ When she picks up the expensive brand of corn, the shelf notes this information. When she puts the can back and places the store brand corn in her cart, the readers in both the

Accenture, Real-World Showroom, http://www.accenture.com/Global/Services/Accenture_Technology_Labs/R_and_I/RealWorldShowroom.htm (last visited Feb. 8, 2007). *But see* KATHERINE ALBRECHT & LIZ MCINTYRE, SPYCHIPS: HOW MAJOR CORPORATIONS AND GOVERNMENT PLAN TO TRACK YOUR EVERY PURCHASE AND WATCH YOUR EVERY MOVE 125–26 (Plume 2006) (discussing how voyeurs could use this technology as a way to see what people are wearing under their clothes).

103. For a description of how easily RFID codes in car keys can be stolen and used, see Brad Stone, *Pinch My Ride*, WIRED, Aug. 2006, at 86, available at <http://www.wired.com/wired/archive/14.08/carkey.html>.

104. Bank of America developed the "interactive advertising" system as an ATM of the future. *See* U.S. Patent No. 6,708,176 (filed Apr. 12, 2002) (issued Mar. 16, 2004). However, the system could be useful in any customer service setting (e.g., supermarkets, coffee shops, and theatre box offices). For a discussion of why this automated greeting may not occur in the near future, see Jerry Brito, *Relax Don't Do It: Why RFID Privacy Concerns are Exaggerated and Legislation is Premature*, UCLA J.L. & TECH., 2004, at 18, available at www.lawtechjournal.com/articles/2004/05_041220_brto.php (discussing how the technology is not practical and customers would find it "creepy").

105. IBM developed the "Margaret" project for this specific purpose to be used in banks. *See* IBM—Coming Everywhere near you: RFID, <http://www-03.ibm.com/industries/financialservices/doc/content/landing/884118103.html> (last visited Feb. 8, 2007). The system uses RFID tags to identify highly valued customers and alert managers or bank tellers of their identity. *Id.*

106. Proctor & Gamble developed the "methods for tracking consumers in a store environment," U.S. Patent App. No. 20020161651 (filed Aug. 22, 2001), and NCR Corporation has developed the "automated monitoring of activities of shoppers in a market," U.S. Patent No. 6,659,344 (filed Dec. 6, 2000) (issued Dec. 9, 2003).

shelf and the cart note her preference (most likely sending her a coupon for the expensive corn the following week). Nearing the ice cream, Jane feels a need to buy a pint of her favorite flavor, but then remembers that her health insurance company will see that purchase too. As part of her “Healthy Lifestyles” program, Jane receives a lower monthly premium in return for the insurance company’s ability to track her exercise and nutrition habits.¹⁰⁷

The easiest part of Jane’s day is paying for her groceries. Because RFID tags can be read from a distance, Jane simply pushes the cart out the door (with a reader built into the door), and the amount of the purchases is deducted from her loyalty account.

But when Jane returns to her vehicle, it is gone. She calls the police, who immediately change the status on her vehicle registration to stolen. Since the thief made the mistake of using the interstate, the police know that he entered the freeway heading south twenty minutes ago. From there, the TrafficLinx system¹⁰⁸ automatically notifies the officer nearest the projected location of the stolen car. The thief is then apprehended within ten minutes, and Jane has her car back before the end of the afternoon.

In order for Jane’s day to become a reality, two future developments are necessary: (1) RFID tags in all consumer products (in the form of the EPC); and (2) RFID tags in license plates and readers along highways. The EPC is becoming a reality, as Marks & Spencer, a British retailer, has already fitted over thirty-five million products with RFID tags.¹⁰⁹ In addition, the roads around Houston, Texas already have RFID readers every one to five miles on the interstates to read RFID toll-paying tags.¹¹⁰ Therefore, while Jane’s

107. While this may seem an extreme use of grocery shopping habits, a more primitive version of this program already exists in Washington state for King County employees. Under the “Healthy Incentives” program, county employees receive a lower monthly premium if they agree to keep a daily journal of their exercise and nutritional habits. See King County, Focus on Employees, <http://www.metrokc.gov/employees/Healthyincentives/default.aspx> (last visited Feb. 8, 2007). For another purpose of tracking grocery purchases, see *Police Officer Fired for Smoking Tobacco*, PORTSMOUTH HERALD (N.H.), June 22, 2003, available at http://www.seacoastonline.com/2003news/06222003/south_of/35552.htm (noting that in Massachusetts it is illegal for police officers and firefighters to smoke tobacco on or off duty).

108. See *supra* note 100.

109. Claire Swedberg, *Marks & Spencer to Tag Items at 120 Stores*, RFID JOURNAL, Nov. 16, 2006, <http://www.rfidjournal.com/article/articleview/2829/1/1>.

110. For a description and photographs of this system, see Houston’s TranStar AVI Traffic Monitoring System, <http://traffic.houstontranstar.org/aviinfo/avi-tech.html> (last visited Feb. 8, 2007).

story may be a vision of the future, it is a vision that is certainly possible.

B. The Legal Implications of Jane's World

When analyzing the uses of RFID technology in Jane's world, the easiest place to start is with those uses that are clearly a search under the Fourth Amendment. Since in the near future all consumer products may have RFID tags, government officials could use an RFID reader to determine whether a specific item is within a home (e.g., a specific stolen gun or television). A search such as this would require a warrant under the Fourth Amendment because the use of an RFID reader in this manner would allow an officer to collect information from inside a home that could not otherwise be perceived with the officer's five senses.

On the other hand, under federal law, once an RFID tag is thrown away, the police are free to use an RFID reader on a person's trash without a warrant.¹¹¹ However, as previously mentioned, states are free to construe their own constitutions as more stringent than the Fourth Amendment.¹¹² California had previously construed its own constitution to protect searches of one's trash.¹¹³ Like the rule regarding pen registers,¹¹⁴ this rule was removed by Proposition 8 (Right to Truth-in-Evidence).¹¹⁵

As previously discussed,¹¹⁶ once private information has been exposed to a third party (or the public), the information is no longer considered private and the government may use the information without first getting a warrant.¹¹⁷ Therefore, barring a legislative act stating otherwise, in Jane's world, this rule would cover three different sets of data.

First is Jane's home personal assistant, which catalogs and tracks all RFID-embedded items in her house and stores this information in a third party's database. Following the holding of

111. *See* *California v. Greenwood*, 486 U.S. 35, 40 (1988) (noting that there is no reasonable expectation of privacy once an item has been placed in the garbage and put to the curb for pickup by a third party).

112. *Id.* at 43.

113. *People v. Krivda*, 486 P.2d 1262, 1268–69 (Cal. 1971).

114. *See supra* note 93.

115. CAL. CONST. art. I, § 28(d).

116. *See supra* text accompanying notes 82–87.

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

Jacobsen would lead to the conclusion that this information could be requested and used by government officials without a warrant, since this previously private information had already been released to a third party.¹¹⁸ On the other hand, if the government were to use an RFID reader to see what was in Jane's house, the officials would need a warrant to make the search valid. Thus, the government could use these third party databases to directly circumvent the Fourth Amendment warrant requirement.

Second are Jane's grocery buying habits, which, like her home inventory, would be open to federal inquiry since she had previously made this information available to a third party (the grocery store).

Third are Jane's whereabouts and driving patterns. Under *United States v. Knotts*,¹¹⁹ the police using RFID technology to merely augment their senses and track people would not be a "search" under the Fourth Amendment.¹²⁰ However, the scenario in Jane's world (with RFID tags on every vehicle and readers at every interstate entrance and exit ramp) may be the type of situation that the Court in *Knotts* said would require a different legal conclusion.¹²¹

Thus, there are two sides in determining whether a widespread vehicle identification system (which would allow officials to track Jane's whereabouts and driving patterns) would be a search under the Fourth Amendment. On one side, law enforcement officials maintain that the use of RFID tags and readers is nothing more than increasingly efficient police work.¹²² The police *could* have an officer at every on and off ramp, writing down the license plates of vehicles. Instead, the police will use RFID readers to conduct essential police work more efficiently (much like using red light and speeding cameras instead of posting a police officer at every signal light).

On the other hand, following one car (as was done in *Knotts*) is vastly different from following every vehicle in a metropolitan area. The TrafficLinx system in Jane's world is exactly the twenty-four

118. However, a state may have stronger protections than the federal law. For example, in California, Section 1 of Article 1 of the California Constitution provides for the "inalienable right" to privacy. This right has been construed to apply to all actors—state and non-state. *Hill v. Nat'l Collegiate Athletic Ass'n*, 865 P.2d 633, 642–43 (Cal. 1994).

119. 460 U.S. 276 (1983).

120. *Id.* at 282–83.

121. *Id.* at 283–84.

122. *Id.* at 276.

hour surveillance situation that the defendant in *Knotts* tried to argue against.¹²³ The police would be able to track every vehicle on every interstate during every hour of the day, in effect creating a comprehensive scheme that greatly exceeds the technology contemplated in *Knotts*.

While the Court may consider such a system an unreasonable search, this issue may not arise for more than fifteen years after RFID is integrated into society.¹²⁴ However, this conclusion is not guaranteed. As discussed, the Court could decide that RFID technology merely augments the authorities' five senses (and thus is not a search under the Fourth Amendment).

Since the constitutional debate is not a settled issue, a societal debate must occur in order for the rights of the people to be protected. Citizens, corporations, and legislatures must ask two main questions. First, does our society want these types of future RFID uses? Second, if these uses are not desired, what actions can be taken to limit the development and improper use of such technologies so that society's privacy needs are properly protected?

V. PROTECTING OUR PRIVACY: A THREE-PRONGED APPROACH

The duty to protect individuals from an unchecked use of RFID technology that exceeds the expectations of society falls on no singular group or entity. Instead, thoughtful and proper action must occur at each and every level of society: legislative oversight, private/public sector restraint, and consumer awareness.

A. Legislative Oversight: Reflecting and Then Carefully Wading into RFID Technology

So far, Congress has not enacted federal legislation to specifically regulate RFID technology. In fact, according to one industry expert, the time is still too early and the technology too young to legislate on RFID.¹²⁵ In addition, a Federal Trade

123. *Id.*

124. An example of this delayed reaction would be radio transponder technology, a cousin of RFID. In 1968, Charles Fried wrote an article on the privacy concerns and effects of radio transponders. Charles Fried, *Privacy*, 77 *YALE L.J.* 475, 475-76 (1968). It was not until 1983 that the U.S. Supreme Court ruled on the constitutionality of "searches" using radio transponders in *Knotts*, 460 U.S. at 278.

125. *RFID Technology: What the Future Holds for Commerce, Security, and the Consumer: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm.*

Commission report stated that the main protector of privacy issues should be industry participants, not federal legislators or regulators.¹²⁶

However, while federal legislative action has been mostly non-existent, thirteen state legislatures have either proposed or enacted legislation limiting the use of RFID.¹²⁷ The most publicized of these acts was a Wisconsin bill (signed into law in 2006) which makes it illegal for any person to be required to have an RFID tag implanted into their body.¹²⁸ In Rhode Island, a bill forbidding state agencies from requiring RFID tags to be used by employees or schools was passed but vetoed by the governor.¹²⁹ In Texas, a bill was proposed (but not enacted) that would make it illegal to require students to carry RFID tags in schools.¹³⁰

While these state efforts are a good start, in many ways, the industry expert is correct: it is still early for RFID-specific legislation.¹³¹ In addition, efforts at the state level differ greatly. This creates a difficult scenario for producers of RFID technology, where one level of compliance is necessary in state *A* and a completely different level may be necessary in state *B*.¹³² As suggested in the hearings, the best route for legislation at this point is to control the data that RFID tags convey, both at the micro level (one product's journey through the production cycle) and the macro level (aggregate numbers on sales for marketing purposes).¹³³ That

on *Energy and Commerce*, 108th Cong. 57 (2004) (statement of Sandra R. Hughes, Global Privacy Executive, Procter & Gamble Company).

126. FED. TRADE COMM'N, RADIO FREQUENCY IDENTIFICATION: APPLICATIONS AND IMPLICATIONS FOR CONSUMERS 22 (2005).

127. See Posting of Lawton Jordan, RFID Legislation: What You Need to Know About the Debate, to RFID Law Blog (Sept. 20, 2006), <http://rfidlawblog.mckennalong.com/archives/state-legislation-rfid-legislation-what-you-need-to-know-about-the-debate.html>.

128. WIS. STAT. § 146.25 (2006).

129. H. 5929, Gen. Assem., Jan Sess. (R.I. 2005).

130. H.B. 2, 79th Sess. (Tex. 2005).

131. A perfect example would be Wisconsin's statute forbidding the required implanting of RFID tags. Implanted RFID tags could become obsolete over the next few years, in which case the Wisconsin legislature acted much too soon. Conversely, a valid and compelling government justification could be created for requiring implanted RFID tags. In that case, the Wisconsin legislature would then have to repeal their previous act. Either way, Wisconsin may have acted too soon.

132. See *RFID Technology*, *supra* note 125, at 68 (prepared statement of Grocery Manufacturers of America).

133. See *id.* at 25 (statement of Paula J. Bruening, Staff Counsel, Center for Democracy & Technology).

way, issues like Jane Doe's grocery shopping habits and home inventory can be regulated much like her banking information.¹³⁴

Two current actions Congress could take are to amend the ECPA¹³⁵ and the Privacy Act of 1974¹³⁶ to accommodate RFID technology. Amending the Privacy Act of 1974 would require that "fair information practices"¹³⁷ apply to information relayed using RFID technology. These practices include not disclosing a person's private information without the consent of the individual and allowing individuals access to their own records.¹³⁸ Another positive step could have been the "Opt Out of ID Chips Act," which was proposed in 2004 but never enacted.¹³⁹ This bill proposed requiring producers to notify consumers that a product contained an RFID tag and giving consumers the choice to disable the RFID tag at the point of sale.¹⁴⁰ In addition, regulators should seriously listen to public comments about RFID technology and not disregard privacy concerns.¹⁴¹

Moreover, if the U.S. Supreme Court ever held that a particular government use was not a search and that decision was found contrary to society's expectations, Congress could pass legislation

134. See, e.g., 15 U.S.C. § 6802 (2000) (creating a notice requirement from banks to consumers and a higher standard for privacy than currently applies to RFID-enabled information).

135. See Oleg Kobelev, *Big Brother on a Tiny Chip: Ushering in the Age of Global Surveillance Through the Use of Radio Frequency Identification Technology and the Need for Legislative Response*, 6 N.C. J.L. & TECH. 325, 339-40 (2005) (discussing how the Electronic Communications Privacy Act could be amended to include RFID-enabled data under "communications").

136. See John M. Eden, *When Big Brother Privatizes: Commercial Surveillance, the Privacy Act of 1974, and the Future of RFID*, DUKE L. & TECH. REV., Aug. 31, 2005, ¶ 29, at 19-20, available at <http://www.law.duke.edu/journals/dltr/articles/PDF/2005DLTR0020.pdf> (suggesting that the Privacy Act of 1974 be amended to specifically prohibit privacy corporations from collecting excessive amounts of personal consumer data under the "fair information practices").

137. See 5 U.S.C. § 552a (2000).

138. *Id.*

139. H.R. 4673, 108th Cong. (2004).

140. *Id.*

141. When the State Department considered using electronic passports (embedded with an RFID tag), they opened the proposal up for comment. During this comment period, 2335 comments were received, 98.5% of which were *negative* comments. Electronic Passports, 70 Fed. Reg. 61553, 61553 (Oct. 25, 2005) (to be codified at 22 C.F.R. pt. 51). The proposal was nonetheless approved and implemented. *Id.* For an interesting solution to defeat a RFID passport (for example, hit it with a hammer), see Jenna Wortham, *How To: Disable Your Passport's RFID Chip*, WIRED, Jan. 2007, at 46, available at <http://www.wired.com/wired/archive/15.01/start.html?pg=9>.

overriding the Court's precedent (as it did with pen registers).¹⁴² Admittedly, this process would be reactive to the demands and needs of society, not prospective as some privacy advocates would prefer.¹⁴³

In the meantime (the time between prospective and reactive actions), two large groups can take matters into their own hands to help guide society into an era of proper RFID use: those that create the technology (private/public sector) and those who are affected by the technology (consumers).

B. Private and Public Sector Restraint: A Beginning but Not an End

As the Federal Trade Commission report noted, the RFID industry must play an important role in addressing the privacy concerns that come with RFID technology.¹⁴⁴

Currently, some of the RFID patents secured by corporations have scary names, such as “[i]dentification and tracking of persons using RFID-tagged items.”¹⁴⁵ Another inventor has developed a system that uses an RFID-enabled armband.¹⁴⁶ The function of this armband is to deliver, with the push of a button, “an immobilizing dosage of a[n] . . . anesthetic.”¹⁴⁷ The inventor even envisioned this product being used on a large group, capable of disabling multiple individuals at once.¹⁴⁸ In addition, one artist/activist developed an imaginary weapon: a sniper rifle capable of delivering an implantable RFID tag from 1100 meters away without the target knowing what happened.¹⁴⁹ This artist was able to infiltrate a 2002 Chinese weapons show and even had several governments interested in his prototype rifle.¹⁵⁰

142. *See supra* notes 88–92 and accompanying text.

143. *See* Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), RFID Right to Know Act of 2003, <http://www.nocards.org/rfid/rfidbill.shtml> (last visited Feb. 8, 2007).

144. *See* FED. TRADE COMM’N, *supra* note 126, at 22.

145. U.S. Patent Application No. 20020165758 (filed May 3, 2001) (issued Nov. 7, 2002).

146. U.S. Patent Application No. 20030071734 (filed Sept. 23, 2002) (issued Apr. 17, 2003).

147. *Id.*

148. *Id.*

149. Empire North, http://www.backfire.dk/EMPIRENORTH/newsite/products_en001.htm (last visited Feb. 8, 2007).

150. *See id.*

Obviously, concerns about the abuse of RFID technology are not reduced by inventions such as these. To help consumers embrace RFID technology, producers should pursue only those uses where the benefits of RFID greatly exceed the individual privacy concerns.

One group that may be following this philosophy is the Department of Homeland Security. In a draft report, one committee stated that in certain human tracking uses, “RFID appears to offer little benefit when compared to the consequences it brings for privacy and data integrity.”¹⁵¹ The report then recommended that while RFID is a useful tool for tracking materials, it should be disfavored in terms of tracking humans.¹⁵²

In terms of private sector restraint, most producers have been unwilling to give up using such a promising new technology, despite the privacy concerns. A few companies have stopped using item-specific RFID tags in products due to consumer complaints.¹⁵³ However, for the most part, companies have attempted to quietly roll out RFID-tagged items.¹⁵⁴

In order for RFID to be accepted, consumer products companies must follow their own industry standards. Under the EPCglobal “Guidelines on EPC for Consumer Products,” there are four principles that guide the development and use of RFID technology: security, consumer notice, consumer choice, and consumer education.¹⁵⁵ Security refers to the proper use, storage, and protection of consumer data, both on the aggregate and individual level—keeping data protected to the full protection of state and federal law.¹⁵⁶ Consumer notice is achieved by clear and effective labeling of all products that contain an item-level RFID tag.¹⁵⁷ On

151. DEP’T OF HOMELAND SEC., THE USE OF RFID FOR HUMAN IDENTIFICATION: A DRAFT REPORT FROM DHS EMERGING APPLICATIONS AND TECHNOLOGY SUBCOMM. 1 (2006), available at http://www.aeanet.org/governmentaffairs/DHS_RFID_in_Humans_Paper0506.asp.

152. *Id.* at 10–11.

153. See Mark Roberti, *A Setback for RFID?*, RFID JOURNAL, Apr. 14, 2003, <http://www.rfidjournal.com/article/articleview/382/1/1/> (discussing Benetton’s attempts to tag one line of clothing and the subsequent privacy debate).

154. See ALBRECHT & MCINTYRE, *supra* 102, at 37–53 (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).

155. EPCglobal, Guidelines on EPC for Consumer Products, http://www.epcglobalinc.org/public/ppsc_guide/ (last visited Feb. 8, 2007).

156. *Id.*

157. *Id.*

some initial tags, the EPC notification was smaller than one-half inch and not in the form of an industry standard icon.¹⁵⁸ Notification must be clear and conspicuous so that consumers can make an educated choice. In terms of consumer choice, they must be given the option to “kill” or discard the RFID tag at the point of sale with no negative consequences.¹⁵⁹ The last requirement, consumer education, will be discussed in the following section.

*C. Consumer Awareness: The Key to
Understanding and Implementing RFID Technology*

In a study of 8500 adults conducted in April 2005, only 41% of those questioned had even heard of RFID technology.¹⁶⁰ This was an improvement from the survey six months earlier, where only 28% had heard of RFID.¹⁶¹ Of those surveyed in April 2005, 65% were concerned about privacy issues, including 25% that were “very concerned.”¹⁶² Interestingly, adults who knew more about RFID technology were actually less concerned about privacy issues than those who had not heard of RFID.¹⁶³

What does this mean about the adoption and implementation of RFID technology? Simply put, how can a society decide whether a technology is good or “right” for it, if the society does not even know what the technology is? Both RFID proponents and privacy advocates say that better education is the key to society accepting RFID technology.¹⁶⁴

The RFID industry can easily take the first step in this education campaign by providing accurate information about the uses and capabilities of RFID technology. Instead of downplaying and covering up RFID uses,¹⁶⁵ companies should discuss the current

158. See ALBRECHT & MCINTYRE, *supra* 102, at 236.

159. As previously mentioned, these two principles (consumer notification and consumer choice) were also the basis for the “Opt Out of ID Chips Act,” which was proposed, but never enacted, in the U.S. House of Representatives. H.R. 4673, 108th Cong. (2004); see also *supra* text accompanying notes 128–29.

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

161. *Id.*

162. *Id.*

163. *Id.*

164. See EPCglobal, *supra* note 155; ALBRECHT & MCINTYRE, *supra* 102, at 222.

165. See ALBRECHT & MCINTYRE, *supra* 102, at 156–57 (noting how RFID industry marketing companies are using euphemisms, e.g., “radio barcodes,” “green tags,” and

limitations of RFID technology. That way, when new uses or increased technology arrives, consumers will be better equipped to decide whether this new technology is necessary and “good” for society.

On the consumer side, individuals need to take an active role in educating themselves. If consumers wait until Jane Doe’s world is a reality, consumer outcry will be too late. Instead, the dialog about RFID must take place before the system is fully implemented. Currently, only a few companies (e.g., Marks & Spencer, Wal-Mart, and Tesco) have developed item-specific RFID tagging.¹⁶⁶ However, in the coming years, as the price for an individual tag drops below ten cents, more companies will be tagging individual items.

Thus, now is the time for consumer-driven awareness programs and debates over whether the technology is “good.” If society waits until RFID technology becomes prevalent, such a debate will be rendered moot.

VI. CONCLUSION

In the coming years, RFID technology is poised for massive growth.¹⁶⁷ Under the Fourth Amendment and U.S. Supreme Court jurisprudence, very few potential government uses for the technology would require the use of a warrant. In addition, there are many technologies that are being developed that society would probably prefer did not exist. Therefore, only through a combination of increased consumer education, restraint by both the private and public sectors, and proper legislative oversight can RFID technology be effectively implemented into our society.

The concerns of privacy advocates about RFID technology creating a “Big Brother” may be years and several technology leaps away. However, with the technology poised to increase in availability and decrease in price, now is the time for dialogue. “[I]llegitimate and unconstitutional practices get their first footing . . . by silent approaches and slight deviations from legal

“contactless smart cards,” to describe RFID tags in light of negative consumer feedback to the phrase RFID tags).

166. *See id.* at 223–24; Swedberg, *supra* note 109.

167. *See* WYLD, *supra* note 4, at 8 (projecting the RFID market to be worth \$25 billion by 2015).

Winter 2007]

RFID TECHNOLOGY

879

modes of procedure”¹⁶⁸ Thus, it must be the duty of all citizens (government, corporate, and individual alike) to assure that such an undesirable and stealthy encroachment on individual Fourth Amendment rights does not occur.

168. *Schneekloth v. Bustamonte*, 412 U.S. 218, 228 (1973) (internal quotation marks omitted).

