UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 6
Issue 2 *Spring 2005*

Article 4

3-1-2005

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

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

Oleg Kobelev[1]

I. Introduction: You Can't Run and You Can't Hide

One of the most controversial provisions of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act") allows the government to track the books people check out of the library.[2] The critics of this provision argue that allowing the government to monitor what books people read is an unprecedented invasion of privacy that will erode civil liberties and chill free speech.[3] These critics may be surprised to learn that rapid advances in Radio Frequency technology put the private sector, not the government, on the verge of what can be described as a massive bugging program. The culprit is a tiny microchip called a Radio Frequency Identification ("RFID") tag that can be inserted into everyday household items, thus allowing the government, or, for that matter, virtually anybody with a scanner to track the physical location of every carton of milk, every child's toy, and every pair of socks that consumers buy. Compared to the

---

[1] J.D. Candidate, University of North Carolina School of Law, 2006.

[2] USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287, 50 U.S.C. §§ 1861–1862 (2004) (allowing the FBI to compel production of library circulation records as a part of business records).

[3] *See generally* Kathryn M. Martin, Note, *The USA PATRIOT Act's Application To Library Patron Records*,, 29 J. LEGIS. 283 (2003); Jeremy C. Smith, Comment, *The USA Patriot Act: Violating Reasonable Expectations of Privacy Protected by the Fourth Amendment Without Advancing National Security*, 82 N.C. L. REV. 412 (2003); Ann Beeson and Jameel Jaffer, ACLU, *Unpatriotic Acts: The FBI's Power to Rifle Through Your Records and Personal Belongings Without Telling You*, *at* http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=13246&c=206 (July 2003) (on file with the North Carolina Journal of Law & Technology).

potential privacy threats stemming from the unrestricted use of these tags, the much feared "sneak-and-peak" provisions of the USA PATRIOT Act look like child's play.

RFID is a technology that allows companies and governments to implant tiny and virtually undetectable microchips or "tags" with antennas into almost any product or animal, including humans. Predicted by MIT researchers to become the most pervasive computer technology in history,[4] most RFID tags do not require any external power source and can transmit information via radio waves when the tag enters the reception field of the nearest scanner.[5] RFID tags are commonly used to store an Electronic Product Code ("EPC") that assigns a unique identifier to every RFID chip, thereby allowing fast, efficient, and cost-effective inventory tracking.[6]

The benefits of RFID technology are obvious. The technology allows for faster checkout times at the grocery store, significant cost-savings for the companies who can now track their inventories more efficiently and at a lower cost, and lower prices for the consumers as companies reduce their overhead costs. The potential dangers of the misuse of the technology, however, are much harder to identify with any precision given the relative infancy of the technology and the lack of response from the industry.[7]

The very real danger that unregulated, unrestricted use of RFID technology poses to privacy is the central theme of this article. The State Department's plans to embed all US passports with RFID chips by late 2005[8] and the news of the Mexican

---

[4] Sanjay E. Sarma et al., *Radio Frequency Identification: Security Risks and Challenges*, 6 RSA LABORATORIES CRYPTOBITES 2 (2003).

[5] *Id.* at 4.

[6] *Id.*

[7] *See* Alien Technology Corporation, *at* http://www.alientechnology.com/ (last visited Apr. 13, 2005) (on file with the North Carolina Journal of Law & Technology). Alien Technology Corporation is arguably the world's largest manufacturer of RFID chips. It has so far failed to mention anything about the privacy concerns surrounding the use of RFID on its website or in its press releases, speeches, or training manuals. This author's repeated requests for comments on this failure have so far gone unanswered.

[8] *See* Susan Llewelyn Leach, *Passports Go Electronic With New Microchip*,

government implanting their workers with RFID chips as a means of accessing restricted areas inside government buildings[9] demonstrate the urgent need for closer examination of potential abuses of RFID technology and ways to prevent such abuse.

This Recent Development seeks to accomplish four main objectives. First, it describes the nature of RFID technology, and the risks that RFID technology poses to our privacy by greatly enhancing location-tracking capabilities of the government, the companies that use the technology and ordinary criminals that may abuse it. Second, this Recent Development examines the precise nature of the privacy rights threatened by RFID technology by discussing the concept of location privacy—a new understanding of privacy as freedom of an individual from having his or her movements monitored without their consent. Third, this Recent Development demonstrates that existing constitutional and legislative frameworks are not designed to protect location privacy from unauthorized privacy violations. Finally, this Recent Development proposes legislative solutions, including incorporating the concept of location privacy into the Electronic Communications Privacy Act, regulating RFID technology through the Federal Communications Commission pursuant to its authority over public airwaves, and requiring encryption mechanisms in the RFID tags themselves.

II. Privacy and RFID Technology: Big Threat from a Little Bug

The origins of RFID technology lie in the Universal Product Code systems used by manufacturers and retailers to keep track of their inventories.[10] At its core, RFID technology is a natural progression from the familiar optical bar-code technology

---

CHRISTIAN SCI. MONITOR, Dec. 9, 2004, at 12, *available at* http://www.csmonitor.com/2004/1209/p12s01-stct.html.

[9] *See* Will Weissert, MSNBC News, *Microchips Implanted in Mexican Officials*, *at* http://www.msnbc.msn.com/id/5439055/ (July 14, 2004) (on file with the North Carolina Journal of Law & Technology).

[10] Uniform Code Council, Inc., *Universal Product Code*, *at* http://www.uc-council.org/upc_background.html (last visited Apr. 13, 2005) (on file with the North Carolina Journal of Law & Technology).

currently used in five billion scans a day.[11] The existing optical bar technology incorporates two different standards—a one-dimensional bar code used by most manufacturers and two-dimensional bar codes used by shipping companies such as the United States Postal Service and United Parcel Service ("UPS").[12] Unlike these optical codes, RFID auto-identification systems have two critical advantages: Each chip is assigned its own unique electronic identifier (whereas a one-dimensional bar code only allows enough data to identify a broad category)[13] and data can be read outside the line of sight and through objects such as walls. In other words, data can be read even if the chip is stacked inside a box on the top shelf in a warehouse. The items do not need to be scanned manually.

RFID technology is not new—it has been widely used in microchips, the manufacturing of automobiles, and even herding cattle.[13] The basic design is very simple and consists of two main elements: the RFID tag itself, a microchip with a data storage capability wired to an antenna coil, and an RFID scanner, a transmitter that interacts with the chips' writing to modify the information on the chip. The information from the scanner is generally sent to a computer database that keeps track of the data and associates each code with the product it describes.[14] Another important feature of RFID tags is that they are passive and usually do not require an external power source to keep them operational.[15] The microchip inductively receives power whenever its antenna receives a radio-impulse from the scanner as if the scanner "shouts" to the passive tag, bringing it to life and allowing transmission.[16] While the current range of the scanners is limited to two to five feet on passive tags, this range can be greatly

---

[11] *Id.*

[12] *See* The Barcode Software Center, *Barcode Symbologies and Label Standards*, *at* http://www.mecsw.com/specs/speclist.html (last visited Mar. 4, 2005) (describing various standards used in the industry) (on file with the North Carolina Journal of Law & Technology).

[13] Sarma et al., *supra* note 4, at 2.

[14] *Id.* at 4.

[15] There are active tags wired to a battery, which allows for much greater range, but due to higher costs they are less widespread. *Id.*

[16] *Id.*

enhanced by developing more powerful and sophisticated scanners or by simply increasing the density of the existing scanners.

The crucial difference between RFID technology "then" and RFID technology "now" is the cost. The recent advances in miniaturization and micro-chip manufacturing have lowered prices so dramatically as to allow RFID chips to currently cost around fifty cents, with MIT's studies projecting the cost to drop to five cents in two to three years.[17] As the price of RFID technology plummets, companies will become more cost-efficient by installing RFID technology into a wider range of products.[18]

It is hard to overstate the benefits of implementing RFID tracking technology. Soon companies will have instant 24-hour-a-day information on the location and quantity of each item in their inventory, as well as the movement of those items through distribution channels. In the ideal world, both retailers and manufacturers will have interoperable online databases instantly tracking the movement of every piece of their inventory at all times. Imagine every retailer and manufacturer, no matter how small, having the same inventory management capabilities as the famously efficient Wal-Mart[19] but at a fraction of the cost.

Nonetheless, the great advantages of RFID technology come with a cost, reaffirming Milton Friedman's famous aphorism that there is no free lunch. The downside, or perhaps the consequence, of low-cost RFID technology is the lack of a viable encryption mechanism to protect the data on the chip from unintended use. Low power consumption, slow read rates, as well as the storage and computing capacities of RFID chips all fall far below the requirements for encryption systems used on microchips elsewhere.[20] Thus, various "phishing"[21] techniques that are rapidly

---

[17] *Id.* at 3–5.

[18] *Id.* at 2–3.

[19] *See The Wal-Mart Empire: A Simple Formula and Unstoppable Growth*, RESEARCH AT PENN, *at* http://www.upenn.edu/researchatpenn/article.php?631&bus (Apr. 9, 2003) (describing the efficiency of Wal-Mart operations) (on file with the North Carolina Journal of Law & Technology).

[20] RFID tags generally have about 250 to 1000 security gates (microchip circuits available for encryption), whereas most symmetrical encryption algorithms requires 20,000 to 30,000 security gates. Sarma et al., *supra* note 4, at 5.

gathering steam on the Internet can be modified by computer hackers to extract the contents of RFID chips. It would be even easier for unscrupulous companies to use RFID technology to track customers' buying habits and, as such, conduct their market research cheaply and without the participant's consent. Finally, the government may either commandeer the existing networks or establish their own to conduct its surveillance uninhibited by either legislative or constitutional constraints. Government surveillance may take a variety of forms from matching customers' purchases against computer databases for signs of suspicious activity[22] to tracking a person's physical location as a means of electronic surveillance.

The lack of security combined with a low cost of RFID technology has the potential to fundamentally change the way we view privacy, leading to a world in which our physical location is never safe from the prying eye of the government, companies, or a

---

[21] Phishing is

> the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The email directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

WEBOPEDIA COMPUTER DICTIONARY, *at* http://www.webopedia.com/TERM/p/phishing.htm (last visited Mar. 4, 2005) (on file with the North Carolina Journal of Law & Technology).

[22] The government has already attempted to create a similar system in the context of airline security with the CAPPS II program that was later scrapped because of technical difficulties and privacy concerns. *See* Mimi Hall & Barbara DeLollis, *Plan to Collect Flier Data Canceled*, USA TODAY, July 15, 2004, at 1A, *available at* http://www.usatoday.com/news/washington/2004-07-14-fly-plan_x.htm. CAPPS II as described in 68 Fed. Reg. 45265 (Aug. 1, 2003) was designed to automatically cross-reference the data each passenger provided to the airline companies when purchasing a ticket against a wide variety of governmental, public and commercial databases in order to conduct a risk assessment of the likelihood of that passenger being a security risk. Depending upon the relative score that each passenger received, the database would automatically flag the passengers with elevated scores for additional screening at the airports or, in some circumstances, for immediate detention.

hacker. As RFID technology proliferates, it will literally surround future consumers wherever they go and whatever they do. While RFID technology is only one of a host of other technological devices that could be abused to violate consumers' location privacy,[23] it has three critical differences not found in other technologies that make it a true "über-bug": low price, passivity (not requiring external power source), and very small size. While one can conceivably turn off his or her cell phone and disable GPS devices, RFID chips cannot be turned off or even easily found due to their miniature size. Therefore, it is particularly disturbing that no effective constitutional or legal constraints currently exist to protect consumer privacy from the threat that this technology represents.

III. Location Privacy and the Constitution: The Steep Road to Nowhere

The concept of privacy has developed slowly in the United States. While there is no direct mention of the word privacy in the Constitution, common law in both the United States and England sought to punish eavesdropping.[24] While the passage of the Fourth Amendment outlawed "unreasonable searches and seizures,"[25] carried out by government actors and the Fifth Amendment prohibited compelling self-incrimination,[26] the exact contours of how these protections related to eavesdropping remained unclear.

---

[23] *See generally* Laurie Thomas Lee, *Can Police Track Your Wireless Calls? Call Location Information and Privacy Law*, 21 CARDOZO ARTS & ENT. L.J. 381 (2003) (reviewing privacy threats from the use of cell phones); Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349 (2004).

[24] "Eavesdroppers, or such as listen under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales, are a common nuisance and presentable at the court-leet; or are indictable at the sessions, and punishable by fine and finding of sureties for [their] good behavior," 4 BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 169 (1769).

[25] U.S. CONST. amend. IV.

[26] U.S. CONST. amend. V.

In *Olmstead v. United States*,[27] Olmstead, a Seattle bootlegger, challenged his conviction by arguing that government wiretapping should have been suppressed as a violation of his Fourth and Fifth Amendment rights. The Supreme Court, led by Chief Justice Taft, disagreed, holding that Fourth Amendment search and seizure protections did not apply to government wiretapping because no physical trespass had taken place and no actual papers or other tangible evidence were seized.[28] The Court also rejected Olmstead's Fifth Amendment challenge, holding that since he was not compelled to use the phone to offer incriminating evidence, his Fifth Amendment rights were not violated.[29] Similarly, in both *Goldman v. United States*[30] and *On Lee v. United States*[31] the Court continued its insistence that physical trespass was the proper trigger for protections of the Fourth and Fifth Amendments, thus excluding from their reach evidence obtained through electronic eavesdropping by government agents.

This formalistic view first began to unravel in *Silverman v. United States*,[32] where the government inserted a "spike mike" into the common wall of a row house in which the recorded conversation took place.[33] Instead of dwelling on the intricacies of property law in determining whether actual trespass had occurred, the Court held:

> [a]t the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion. . . . But [our] decision here does not turn upon the technicality of a trespass upon a party wall as a matter of local law. It is based upon the reality of an actual intrusion into a constitutionally

[27] 277 U.S. 438 (1928).
[28] *Id.* at 466.
[29] *Id.* at 462.
[30] 316 U.S. 129 (1942) (using a dictaphone to secretly tape conversation in the next office did not violate Fourth Amendment since there was no trespass).
[31] 343 U.S. 747 (1952) (secretly recording a conversation in the public laundry room did not trigger Fourth Amendment protections since the area was open to the public).
[32] 365 U.S. 505 (1961).
[33] *Id.* at 506.

protected area."[34]

Shortly after *Silverman*, the Court dispensed with the notion that trespass to real property was necessary to trigger the protections of the Fourth Amendment altogether. In *Katz v. United States*,[35] a bookie was convicted of using a public phone to take and place bets. His conversations were recorded by a listening device set outside the phone booth. The Court specifically repudiated the *Olmstead* and *Goldman* trespass doctrines, stating that "[t]he fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance."[36] The new expectation-of-privacy based definition that emerged consisted, in Justice Harlan's words, of 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.'"[37]

Despite the broad language of *Katz* and the attendant requirement of warrants for government wiretapping, the Court's decision has been largely limited to the contents of the conversation, rather than giving any meaningful protection from the government tracking the physical location of an individual—the concept referred in this article as location privacy. Thus, the federal courts have not yet recognized "location privacy" as falling within the "reasonable expectation of privacy" prong of the *Katz* analysis. Almost every case challenging the propriety of warrantless government surveillance of a persons' physical location has been rebuked by the courts as outside the scope of the protections of the Fourth Amendment.

In a harbinger of things to come, the Supreme Court held in *Smith v. Maryland*[38] that there was no expectation of privacy in dialing phone numbers. In *Smith*, police used a pen register (a device used to record numbers dialed from a particular telephone and identify their location) to record numbers from a home of the

[34] *Id.* at 511–12.
[35] 389 U.S. 347 (1967).
[36] *Id.* at 353.
[37] *Id.* at 361 (Harlan, J., concurring).
[38] 442 U.S. 735 (1979).

man thought to be threatening a robbery victim.[39] The court held that using a pen register did not constitute search and seizure within the meaning of the Fourth Amendment, because there was no expectation of privacy in dialing phone numbers.[40] In what has now become a standard justification for refusing to incorporate location privacy into the Fourth Amendment, the Court emphasized the voluntary nature of dialing the number, reasoning that Smith "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, [Smith] assumed the risk that the company would reveal to police the numbers he dialed."[41]

In an even more glaring rejection of location privacy, the Court in *United States v. Knotts*[42] found no expectation of privacy when the government attached a radio-tracking device to a canister of chemicals subsequently traced to the house of the defendant. Ominously stating that "[a] person traveling in an automobile on public thoroughfares has *no reasonable expectation of privacy in his movements* from one place to another. . .,"[43] the Court deemed that traditional expectations of privacy do not attach to movements that can potentially be observed through "visual surveillance from public places."[44] In *Knotts* and its progeny,[45] the Court has interpreted the *Katz* rule narrowly, allowing electronic surveillance in virtually all places where a potential for visual observation exists. The only bright spot for location privacy advocates is the Court's consistent recognition of the home as a traditional zone of

[39] *Id.* at 737.
[40] *Id.* at 742–43.
[41] *Id.* at 744.
[42] 460 U.S. 276 (1983).
[43] *Id.* at 281 (emphasis added).
[44] *Id.* at 282.
[45] California v. Ciraolo, 476 U.S. 207, 215 (1986) (holding that aerial observation of the home from 1000 feet by police looking for drugs did not violate Fourth Amendment because "[i]n an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his . . . [drugs] were constitutionally protected from being observed with the naked eye from an altitude of 1000 feet"); Dow Chemical Co. v. U.S., 476 U.S. 227, 238–39 (1986) (using precision aerial mapping camera does not violate Fourth Amendment where the area being watched is more akin to an open field).

privacy,[46] thus forbidding warrantless use of tracking devices inside the house[47] and the use of "peeking technology" to look inside property otherwise hidden from public view.[48]

It is also worth noting that the holding in *Smith* is being increasingly questioned in light of a new test articulated in *Kyllo v. United States*.[49] In *Kyllo*, the Court held that using thermal imaging technology to locate marijuana plants growing inside the defendant's house constituted a search within the meaning of the Fourth Amendment.[50] Under the new *Kyllo* test, the insides of the house are off limits to any technology, no matter how "unobtrusive" the technology may be.[51] Thus, the use of pen registers, which are not in general public use, may be considered unconstitutional under this new test if the phone number is dialed from inside the house.

Overall, under the Court's current reading of the Fourth Amendment, with the limited exception of privacy within one's house, the concept of location privacy has not yet gathered enough legitimacy to be recognized as privacy worth protecting. Despite criticism,[52] the Court continues to insist that the potential for visual observation defeats the reasonable expectation of privacy.

---

[46] *See* Oliver v. United States, 466 U.S. 170, 178 (1984) ("[T]he Court since the enactment of the Fourth Amendment has stressed 'the overriding respect for the sanctity of the home that has been embedded in our traditions since the origins of the Republic.'") (quoting Payton v. New York, 445 US 573, 601 (1980)).

[47] United States v. Karo, 468 U.S. 705, 714 (1984).

[48] *See infra* text accompanying notes 49–51.

[49] 533 U.S. 27 (2001).

[50] *Id.* at 34.

[51] *Id.* at 35–36.

[52] *See* Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 CAL. L. REV. 1593 (1987) (criticizing the court's concept of privacy as too limited and individualistic and arguing that a concept of shared privacy within the confines of a narrow group but limited to the outside world is equally worth protecting); *see also* Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727, 740 (1993) (disputing the Court's finding of no reasonable expectation where one shares information with third parties, and finding that most people surveyed viewed government inspection of their bank records to be highly intrusive and unreasonable).

IV. Location Privacy and Legislative Regulation: Not Seeing the Forest for the Trees

In addition to the constitutional provisions of the Fourth Amendment, the Federal government and virtually all states[53] have enacted statutory provisions dealing with electronic surveillance and wiretapping. While different in coverage, goals, and implementation, these statutes are almost uniform in their rejection of location privacy as being worthy of protection.

The centerpiece of federal legislation in this area is the Electronic Communications Privacy Act ("ECPA") of 1986,[54] the successor to the Title III Omnibus Crime Control and Safe Streets Act of 1968.[55] Among the goals of the ECPA was a desire to update eavesdropping regulations to address current technology and avoid unnecessary restrictions on then emerging fields of communications technology.[56] In 1994, as a response to rapidly changing technology, Congress sought to augment police authority to use the latest electronic surveillance tools by adopting the Communications Assistance for Law Enforcement Act ("CALEA").[57] Furthermore, Congress significantly expanded the government's surveillance and wiretapping authority following the September 11, 2001 terrorist attacks with the passage of the USA PATRIOT Act,[58] the Intelligence Authorization Act for Fiscal Year 2002,[59] and the Department of Homeland Security Act 2002.[60]

In general, the ECPA outlaws various forms of electronic eavesdropping, as well as possession of eavesdropping equipment, and use and disclosure of information obtained via illegal

---

[53] *See, e.g.*, N.C. GEN. STAT. § 15A-287 (2003); N.Y. PENAL LAW §250.05 (2003); CAL. PENAL CODE §631 (wire), 632 (oral), 632.7 (electronic) (2003).
[54] 8 U.S.C. §§ 2510–2521 (2004).
[55] 8 U.S.C. §§ 2510–2521 (1970 ed.).
[56] S. REP. NO. 99-541, at 5 (1986), *reprinted* in 1986 U.S.C.C.A.N. 3555, 3557.
[57] Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in 18 U.S.C. § 2522 (1994), and 47 U.S.C. §§ 1001–1010 (1994)).
[58] Pub. L. No. 107-56, 115 Stat. 272 (2001).
[59] Pub. L. No. 107-108, 115 Stat. 1394 (2001).
[60] Pub. L. No. 107-296, 116 Stat. 2135 (2002).

eavesdropping.[61] The ECPA also establishes separate crimes for unlawful access to stored information,[62] and unlawful use of a pen register or a trap and trace device.[63] At its core, the ECPA outlaws intentional interception or attempts of interception of any wire, oral or electronic communication by using electronic or mechanical devices.[64] However, the ECPA specifically exempts from its definition of communication "any communication from a tracking device"[65] which it subsequently identifies as "[an] electronic or mechanical device which permits the tracking of the movement of a person or object."[66] The rationale behind this specific exclusion evidently stems from the fact that Congress sought to protect the content of the communications as opposed to restricting the physical means with which these communications were captured.[67]

As currently written, the ECPA does not protect location privacy or prohibit unauthorized tracking with RFID devices. The courts have recently confirmed this reading of the statute in *United States v. Forest*,[68] where Drug Enforcement Administration agents turned a suspect's cellular phone into a mobile tracking device, thus revealing his general location.[69] The Court of Appeals for the Sixth Circuit held that neither the ECPA nor the Fourth Amendment required suppression of evidence in the defendant's drug trial.[70]

---

[61] 18 U.S.C. § 2511 (2004).
[62] 18 U.S.C. § 2701 (2004).
[63] 18 U.S.C. § 3121 (2004).
[64] 18 U.S.C. § 2511 (2004).
[65] 18 U.S.C. § 2510(12)(c) (2004).
[66] 18 U.S.C. § 3117 (2004).
[67] *See* Congressional Findings, 801 of Pub.L. 90-351.

> [I]n order to protect effectively the privacy of wire and oral communications, . . . it is necessary for Congress to define . . . conditions under which the interception of wire and oral communications may be authorized, to prohibit any unauthorized interception of such communications, and the *use of the contents* thereof in evidence in courts and administrative proceedings.

Id. (emphasis added).
[68] 355 F.3d 942 (2004), *vacated* by 125 S. Ct. 1050 (2005).
[69] *Id.* at 947.
[70] *Id.* at 950–52; *see also* United States v. NY Telephone Co., 434 U.S. 159

The only piece of legislation that acknowledges location privacy is the Communications Assistance for Law Enforcement Act ("CALEA"),[71] which deals with telephone communications and is not directly applicable to RFID technology. CALEA requires telecommunication carriers to make their equipment capable of transmitting "call-identifying information,"[72] but it also specifically prohibits the use of technology (other than pen registers and similar devices) that would reveal the user's physical location.[73] The interpretation and enforcement of the statute is delegated to the Federal Communications Commission ("FCC"),[74] making the agency responsible for promulgating procedures to ensure compliance. This provides one way in which the existing regulatory framework may be extended to cover RFID technology. Unfortunately, the recent history of the FCC's approach to location privacy casts serious doubt on enacting privacy-friendly policies without prodding from Congress.[75]

In short, all of the existing legislative acts in which Congress addressed the issue of privacy seem to either specifically allow or at least tacitly permit virtually unrestricted tracking and monitoring of individuals by both the government and private actors. When this lack of legislative protection is viewed in combination with the courts' refusal to find an expectation of privacy in a person's physical location outside the home, the

---

(1977) (holding trap and trace devices do not capture contents of the defendant's speech and are therefore outside the scope of Title III protection).

[71] 47 U.S.C. §§ 1002–1021 (2004).

[72] 47 U.S.C. § 1002(a)(2)(A).

[73] *Id.* at § 1002(a)(2)(B).

[74] 47 U.S.C. § 229(a) (2004).

[75] In the area of wireless communications, the FCC has interpreted CALEA to require telecommunications carriers to provide call-identifying information such as location and origin of the call to law-enforcement agencies, thus allowing the tracking of cell-phone users at all times. *See In re* Communications Assistance for Law Enforcement Act, Third Report and Order, 14 F.C.C.R. 16794, 16815 (1999). As a result, privacy advocates argued that FCC was threatening civil liberties by giving the federal government new tools for surveillance. *See* William Mathews, *Privacy Advocates Challenge FBI Cell Phone Tracking*, FED. COMPUTER WK., *at* http://www.fcw.com/fcw/articles/2000/0124/web-privacy-01-24-00.asp (Jan. 24, 2000) (on file with the North Carolina Journal of Law & Technology).

picture that emerges is quite grim. The unconsented monitoring of citizens' whereabouts is perfectly legal.[76] While in the pre-RFID world this situation was tolerable simply due to the limitations and expense of the available tracking technology, the advent of RFID, with its cheap and efficient tracking mechanisms and its ubiquity in the marketplace, greatly magnifies the threat to people's privacy.

V. Solutions: And the Answer is . . .

RFID technology is poised to have a promising future as it gradually replaces the bar code as the identifier of choice for manufacturers and retailers alike, increasing efficiency and lowering prices for consumers. Any solution must strike a careful and delicate balance to protect consumer privacy without threatening the viability and the great potential that this technology holds. Legislative initiative designed to protect location privacy could be one such answer. However, to succeed, this initiative must establish rules that are flexible enough to adapt to the still-fluid technology, vigorous enough to prompt change in the RFID industry, and firm enough to provide the same level of privacy to physical location as is currently afforded to other forms of privacy such as content-based privacy.

I propose a three pronged approach. First, the Electronic Communications Privacy Act ("ECPA")[77] must be amended to specifically include location tracking in the definition of "communications" as defined in the Act.[78] Second, built-in security protections must be required in all RFID tags placed on goods that are sold to the general public. Third, the FCC must be delegated the task of regulating the use of public airwaves by the

[76] The deterrent effect of private causes of action such as trespass claims or tort claims seems dubious at best, given the fact that the subjects are unlikely to bring forth the claims without a showing of significant damages simply due to the inherent costs of civil litigation. It is unclear how RFID tracking can lead to such damages. Furthermore, it is increasingly unlikely that the subjects will even be aware of such tracking in the first place, reducing the deterrent effect further.

[77] 18 U.S.C. §§ 2510–2521 (2004).

[78] *Id.*

RFID devices as to minimize the risks to consumer privacy. The combination of these three measures will outlaw troublesome surveillance and create real-world safeguards against the abuse of RFID technology.

The first prong of the initiative, while seemingly simple, requires the fundamental rethinking of rationales behind the ECPA, which contemplated privacy in terms of contents of communications between persons,[79] not location privacy of a person in a physical environment.[80] The recent attempts by the Supreme Court in *Kyllo v. United States* to reconcile the uses of new technology with the original meaning of the Fourth Amendment[81] should be a sign for Congress to take the lead and extend these protections beyond the narrow confines of one's home. Such Congressional initiative would recognize the broader reality that in an increasingly crowded society, the expectation of privacy flows from privacy found in anonymity in a crowd as much as it does from privacy in one's home.

The second prong, while more technical, is just as important. No matter how tough the privacy laws, leaving the RFID architecture completely open to attack is akin to leaving a door to one's house ajar in hopes that no one will burglarize it. The legal framework protecting location privacy must be fortified with practical measures necessary to make violations of the law

---

[79] *See* Congressional Findings, 801 of PUB.L. 90-351.

> [I]n order to protect effectively the privacy of wire and oral communications, . . . it is necessary for Congress to define . . . conditions under which the interception of wire and oral communications may be authorized, to prohibit any unauthorized interception of such communications, and the *use of the contents* thereof in evidence in courts and administrative proceedings.

Id. (emphasis added).

[80] As it is currently written, ECPA explicitly excludes tracking devices, electronic information stored by financial institution or any communication from a tone-only paging device, 18 U.S.C. § 2510(12) (2004).

[81] In *Kyllo v. United States*, 533 U.S. 27 (2001), the Court held that technology that is not in general use when used to monitor activities inside one's house violates the Fourth Amendment search provisions, regardless of how unintrusive it may be, excluding the evidence gathered from the use of thermal imaging device.

more difficult and less widespread. A wide array of encryption technologies are available to accomplish this task—including killing tags after the purchase is made, encrypting the signal with the timed option to self-destruct, and many others—all seeking to make the illegal surveillance more difficult to accomplish.[82]

Finally, Congress should delegate the task of establishing the rules governing the radio-communication between the RFID tags and the scanners to the FCC. This is important because regulatory agencies have the necessary expertise and experience in developing rules that best achieve the balance of the interests of all the stakeholders in the process. As such, the FCC may be asked to determine the optimal range and frequency of signals allowed for the RFID scanners to use, and perhaps require that placement of the tags and the scanners be clearly marked for the consumers to see, thereby further minimizing the potential of secret surveillance.[83]

VI. Conclusion

RFID technology presents complex issues concerning the delicate balance between privacy, efficiency, technology, and the unintended consequences of its use. While by no means unsolvable, these problems are urgent enough to demand a vigorous and proactive approach, rather than passively reacting to the problems as the technology matures enough to make any coherent regulation impractical or, worse, impossible. One need look no further than the continuous problem of email spam, the futility of all technical and legislative initiatives to curb it, and the

[82] *See* Sarma et al, *supra* note 4 at 7 (2003) (describing these methods and other methods to improve RFID security). *But see* RFID Position Statement, *at* http://www.privacyrights.org/ar/RFIDposition.htm (Nov. 20, 2003) (critiquing these methods as inadequate) (on file with the North Carolina Journal of Law & Technology).

[83] The Presidential control over the FCC pursuant to Exec. Order 12866 has the potential to jeopardize the proper functioning of the FCC as a watchdog of governmental intrusion. Proper Congressional oversight as well as clear rules governing applicability of RFID regulations to all governmental and non-governmental actors may be needed to adequately protect the public.

tremendous costs for both consumers and businesses associated with this problem[84] to recognize the need to regulate emerging technologies early and often for the sake of all the participants involved. Amending ECPA to include location privacy as a form of protected communication, requiring built-in encryption in RFID tags themselves, and giving the FCC regulatory oversight over the use of the technology may help solve the problem before it is too late.

[84] *See* Jonathan Krim, *Spam's Cost to Business Escalates: Bulk E-mail Threatens Communication Arteries*, WASH. POST, Mar. 13, 2003, at A01, *available at* http://www.washingtonpost.com/ac2/wp-dyn/A17754-2003Mar12.