1-1-2007

Tracking RFID

Jonathan Weinberg
Wayne State University, weinberg@wayne.edu

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

JONATHAN WEINBERG[*]

Tracking RFID

Abstract: RFID—Radio Frequency Identification—is a powerful enabling technology with a wide range of potential applications. Its proponents initially overhyped its capabilities and business case: RFID deployment is proceeding along a much slower and less predictable trajectory than was initially thought. Nonetheless, in the end it is plausible that we will find ourselves moving in the direction of a world with pervasive RFID: a world in which objects' wireless self-identification will become much more nearly routine, and networked devices will routinely collect and process the resulting information.

RFID-equipped goods and documents present privacy threats: they may reveal information about themselves, and hence about the people carrying them, wirelessly to people whom the subjects might not have chosen to inform. That information leakage follows individuals, and reveals how they move through space. Not only does the profile that RFID technology helps construct contain information about where the subject is and has been, but RFID signifiers travel with the subject in the physical world, conveying information to devices that otherwise would not recognize it and that can take actions based on that information. RFID implementations, thus, can present three related privacy threats, which this article categorizes as surveillance, profiling, and action.

RFID privacy consequences will differ in different implementations. It would be a mistake to conclude that an RFID implementation will pose no meaningful privacy threat because a tag does not directly store personally identifiable information, instead containing only a pointer to information contained in a separate database. Aside from any privacy threats presented by the database proprietor,

[*] Professor of Law, Wayne State University. I am indebted for the contributions made, when I first began looking at this topic several years ago, by the participants in the Cyberlaw Summer Camp sponsored by Harvard Law School's Center for Internet and Society on August 4–8, 2003; the participants in the Conference on Comparative IP and Cyberlaw at the University of Ottawa on October 4, 2003; and by the organizers of, and the participants in, the Conference on Securing Privacy in the Internet Age, held at Stanford Law School on March 13, 2004. I owe special thanks to Jessica Litman and Lee Tien.

privacy threats from third parties will depend on the extent to which those third parties can buy, barter, or otherwise gain database access. Where a tag neither points to nor carries personal identifying information, the extent of the privacy threat will depend in part on the degree to which data collectors will be able to link tag numbers with personally identifying information. Yet as profiling accelerates in the modern world, aided by the automatic, networked collection of information, information compiled by one data collector will increasingly be available to others as well; linking persistent identifiers to personally identifying information may turn out to be easy. Nor are sophisticated access controls and other cryptographic protections a complete answer to RFID privacy threats. The cost of those protections will make them impractical for many applications, though, and even with more sophisticated technology, security problems will remain.

This article suggests appropriate government and regulatory responses to two important categories of RFID implementation. It concludes with a way of looking at, and an agenda for further research on, wireless identification technology more generally.

I. Introduction

RFID—Radio Frequency Identification—is best thought of, one admiring author has suggested, as "some newfangled, infestating, autoreplicating plague."[1] Certainly its use is spreading. The State Department has incorporated RFID into U.S. passports and other U.S. government agencies are moving to include it in other government credentials;[2] banks have distributed tens of millions of RFID-enabled credit cards;[3] truck tires incorporating RFID roll down the highway.[4] Some suggest that the development of RFID marks the beginning of the next fundamental transformation in the history of technology.[5]

Notwithstanding the power and importance of RFID technology, though, its proponents initially overhyped its capabilities and failed to connect that hype with any plausible business case. Efforts to build RFID into inventory control mechanisms for consumer goods are slowing[6]; hardware suppliers are operating at a loss, banking on a payoff down the road.[7] The Department of Homeland Security has recently abandoned plans to incorporate RFID into one key immigration document and declined to order its inclusion in state driver licenses.[8] Some of the most ambitious ideas that entrepreneurs and bureaucrats had for RFID a few years ago—the Transportation Security Agency's notion that RFID-tagged airline boarding passes could allow security personnel to track all passengers' whereabouts, in real time, throughout every airport,[9] or a private-sector plan for a

[1] Bruce Sterling, Shaping Things 88 (2005).

[2] *See infra* notes 109–23, 133–37 and accompanying text.

[3] *See infra* notes 79–80 and accompanying text.

[4] *See infra* notes 71–73 and accompanying text.

[5] *See* Sterling, *supra* note 1, at 8–14 and 88–95.

[6] *See infra* notes 29–70 and accompanying text.

[7] *See* Raghu Das, *Pallet and Case Tagging for Retailers: Q4 Review*, IDTechEx, Nov. 17, 2006, http://www.idtechex.com/products/en/articles/00000503.asp.

[8] *See infra* notes 124–32, 137–43 and accompanying text.

[9] Bob Brewin, *TSA Eyes RFID Boarding Passes to Track Airline Passengers*, Computerworld, Apr. 1, 2004, http://www.computerworld.com/newsletter/0,4902,91830,00.html.

"secure, subdermal RFID . . . payment technology" involving chips implanted in consumers' triceps areas, enabling them to make payments by passing a scanner over their arms[10]—now seem unrealistic or silly. So while RFID will likely still play a crucial and even transformative role in technology development, it will do so on a slower and less predictable trajectory than was initially thought.

RFID deployment—entirely appropriately—has been slowed by important concerns about privacy. Public-interest groups[11] and academics[12] raised alarms over RFID technology early on. Persons carrying RFID-enabled goods or documents, they pointed out, broadcast their tag information to any reader they pass. While RFID tags on tires seem like an effective way of ensuring that the necessary safety information stays tied to the tire,[13] the possibilities for surveillance, once a tire rolling down a highway starts broadcasting its unique ID number, are plain. A wide range of RFID uses have the potential to jeopardize consumer privacy and threaten civil liberties.[14]

In this article, I will examine the trajectory and diffusion—to date, and in the likely near future—of RFID technology. I will consider three sets of privacy threats RFID technology can present (categorized in the paper as the surveillance, profiling, and action threats), and evaluate the circumstances and classes of RFID implementations that

[10] *See* Press Release, Applied Digital Solutions, Applied Digital Solutions' CEO Announces "Veripay™" Secure, Subdermal Solution for Payment and Credit Transactions at ID World 2003 in Paris (Nov. 21, 2003), *available at* http://www.thefreelibrary.com/ Applied+Digital+Solutions'+CEO+Announces+%60%60VeriPay''+Secure,...-a0110394331 ("[O]ne big hurdle remains for RFID systems: security. Lose your RFID-enabled card or earring, and someone else could easily use it to run up charges . . . . The subdermal RFID VeriPay technology specifically addresses the security issue. VeriPay's unique, under-the-skin format offers a much more secure, tamper-proof, and loss-proof solution.") (internal quotation marks omitted).

[11] CASPIAN ET AL., RFID POSITION STATEMENT OF CONSUMER PRIVACY AND CIVIL LIBERTIES ORGANIZATIONS (Nov. 2003), *available at* http://privacyrights.org/ar/RFIDposition.htm (position statement on RFID issued by eight U.S. public interest groups, including such major players as the ACLU and the Electronic Frontier Foundation, and endorsed by others).

[12] *See* Jerry Kang & Dana Cuff, *Pervasive Computing: Embedding the Public Sphere*, 62 WASH. & LEE L. REV. 93, 106–07 (2005); *see also* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004).

[13] *Cf.* Nat'l Tire Dealers & Retreaders Ass'n v. Brinegar, 491 F.2d 31 (D.C. Cir. 1974) (wrestling with the question of how to ensure that a tire's safety information stays available to the consumer once the tire is retreaded).

[14] *See* CASPIAN ET AL., *supra* note 11.

might present each. I will suggest appropriate government and regulatory responses to two important categories of RFID implementation: the inclusion of RFID in government credentials and the use of RFID-enabled inventory control tags. And I will suggest a way of looking at, and an agenda for further research on, wireless identification technology more generally. In the short term, the concrete privacy threats RFID presents are limited. But in the longer term, they are substantial: we may be sliding into a world in which objects' wireless self-identification will become routine, and networked devices will be in a position routinely to collect and process the resulting information. We cannot safely ignore the consequences for privacy.

Section II of the article will explore private-sector deployment of RFID, and Section III will discuss government plans for RFID in identity or immigration documents. Section IV will analyze the privacy threats that various RFID implementations may pose, and Section V will very briefly address why we should care. Section VI will consider potential government and regulatory responses to today's threats, and Section VII will look towards the somewhat more distant future.

II. Private-Sector RFID Deployment

Section II of this article explores private-sector deployment of RFID. It begins with a brief description of RFID technology and the EPCglobal architecture for passive RFID in the supply chain. It sets out the progress to date of RFID tagging for inventory control, and discusses some obstacles to speedy deployment of that technology. It then discusses a variety of other RFID applications and concludes with some observations about RFID deployment to date.

The term RFID describes a family of technologies in which (1) a "tag" contains an integrated circuit storing data that identifies or describes the tag itself, or the item it is attached to, or the person carrying it, and (2) the data can be read, wirelessly, by a separate device called a "reader." The reader, in turn, is part of a system of networked computers that can take action based on the tag data they receive. One RFID implementation in common use today is ExxonMobil's Speedpass technology. The Speedpass wand contains a code uniquely identifying the particular user. A reader in a gas pump or gas station cash register, when near the wand, can detect that code wirelessly. The computer system attached to the reader, armed with the code, can retrieve the user's credit-card information and complete a credit-card transaction charging the user's account for the price of the gas. For purposes of this article, I will include in the RFID category both less expensive technology such as Electronic Product Code ("EPC") Gen2 inventory control tags,[15] and more expensive, more sophisticated technologies such as ISO 14443[16] smart cards.[17]

The distance at which RFID information can be read is a function of the particular technology used. Variables include the choice of operating frequency, the tag design, the reader design, and the level of external interference. In "passive" tag implementations, where the tag itself has no internal battery and gets its power from the reader's signal,[18] the limiting factors include the size of the tag antenna (and thus the tag's antenna gain) and the power the tag's integrated circuit needs in order to operate, as well as the reader's transmission power (limited by Federal Communication Commission ("FCC") regulation), its antenna gain (also limited by FCC regulation), and receiver sensitivity. Plugging in realistic numbers and assuming near-term technology, inexpensive passive tag systems using the frequency bands now contemplated appear to have a theoretical maximum distance of about six meters between tag and reader.[19] Distances actually achievable in the field for these tags are typically shorter; one industry expert suggests that a typical operating environment features

[15] An EPC inventory control tag is inexpensive, with only minimal computing capability. It is a passive tag, as described in the next paragraph. On the EPC specification, *see infra* note 23 and accompanying text.

[16] ISO 14443 smart cards incorporate sufficient computing capability to do encryption and robust access control. For the relevant standards documents, see WG8, Standing Document 1: WG8 Projects, Nov. 13, 2007, http://wg8.de/sd1.html.

[17] Most commentators have taken the same approach. *See, e.g.*, DEP'T OF HOMELAND SEC. DATA PRIVACY & INTEGRITY ADVISORY COMM., REP. NO. 2006-02, THE USE OF RFID FOR HUMAN IDENTITY VERIFICATION 2–3 (Dec. 6, 2006), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf; Simson Garfinkel, *RFID Payments at ExxonMobil, in* RFID: APPLICATIONS, SEC., AND PRIVACY 179 (Simson Garfinkel & Beth Rosenberg eds., 2006). Some vendors of more sophisticated technologies urge that only simple and unsophisticated implementations should be referred to as RFID. *See, e.g.*, SMART CARD ALLIANCE, CONTACTLESS SMART CARDS V. EPC GEN 2 RFID TAGS: FREQUENTLY ASKED QUESTIONS (July 2006), http://www.smartcardalliance.org/resources/pdf/EPC_Gen_2_FAQ_FINAL.pdf.

[18] An "active" RFID tag, in contrast, is powered by an internal battery.

[19] *See* RAVI PAPPU, THINGMAGIC LLC, THE PHYSICS OF RFID 19 (2004), *available at* http://www.ethionet.et/NR/rdonlyres/Engineering-Systems-Division/ESD-290Spring-2005/5FE9474C-3365-463A-B1F5-6E9B252356DA/0/lect6.pdf.

a read range of three to five meters.[20] Other tags are engineered for shorter read ranges, but those ranges can vary widely: smart cards bearing the ISO 14443 chip are designed to operate at a range of two to four inches, but are vulnerable to attack from considerably farther.[21]

RFID technology is amenable to a wide range of implementations. The Auto-ID Center at the Massachusetts Institute of Technology led a major technology development and standardization effort aimed at the use of passive RFID in the retail supply chain. It formally wrapped up that work in October 2003, but continued its standards efforts under the EPCGlobal organizational structure.[22] The Auto-ID Center/ EPCGlobal architecture is directed at what was initially RFID's most commercially important private-sector implementation: inventory management. The architecture contemplates that each pallet or case of consumer goods—indeed, each individual retail item—can have affixed a passive RFID tag holding a globally unique EPC that in turn points to an entry in a worldwide distributed database called the Object Name Service.[23] The EPC is designed to serve the same function in the inventory supply chain as a traditional bar code. It extends the bar code's functionality, though, in two ways.

[20] KAREN GUY & SUSANNE BERGLING, FED. TRADE COMM'N, RADIO FREQUENCY IDENTIFICATION: APPLICATIONS AND IMPLICATIONS FOR CONSUMERS AN FTC WORKSHOP 23–24 (June 21, 2004), http://www.ftc.gov/bcp/workshops/rfid/transcript.pdf [hereinafter *FTC RFID Workshop*] (testimony of Daniel Engels, Executive and Research Director, Auto-ID Labs); *see also id.* at 247 (testimony of Jim Waldo, Sun Microsystems Laboratories) (urging that even where cards that have a ten-meter read range in the laboratory, "[o]n the street, you're lucky if you're going to get a meter or two out of them"); PAPPU, *supra* note 19, at 35 (testimony of Manuel Albers, Phillips Semiconductor) (describing six meter read range on inexpensive cards).

[21] *See* Ilan Kirschenbaum & Avishai Wool, *How to Build a Low-Cost, Extended-Range RFID Skimmer* (May 8, 2006), http://www.eng.tau.ac.il/~yash/kw-usenix06/index.html.

[22] RFID Journal, Frequently Asked Questions: EPCGlobal and Auto-ID Labs, http://www.rfidjournal.com/faq/22 (last visited Jan. 13, 2008). EPCGlobal is a joint venture of EAN International and the Uniform Code Council, which administer the bar code system today. *See id.; see also FTC RFID Workshop, supra* note 20, at 269–70 (testimony of Elizabeth Board, EPC Public Policy Action Committee). EPCGlobal continues to develop RFID standards. *See, e.g.*, Press Release, EPCGlobal, EPCGlobal Inc. Ratifies Electronic Pedigree Standard (Jan. 11, 2007), http://www.epcglobalinc.org/about/media_centre/ press_rel/epcglobal_pr_11012006_Electronic_Pedigree.pdf.

[23] *See* EPCGLOBAL, OBJECT NAMING SERVICE (ONS) VERSION 1.0 (Oct. 4, 2005), http://www.epcglobalus.org/dnn_epcus/KnowledgeBase/Browse/tabid/277/DMXModule/706/ Command/Core_Download/Default.aspx?EntryId=299#search=%22ons%201.0%22. The Object Name Service has a hierarchical structure closely analogous to that of the Internet domain name system. Indeed, the root of the ONS will be operated by the company, Verisign, that operates the COM portion of the Internet domain name system.

First, because readers can detect the EPC wirelessly, tags need not be scanned manually. The reader does not need a line-of-sight connection with a tag,[24] and can read multiple tags at one time. In theory, if each widget were tagged with an EPC, one could place a reader near any of the billion sealed boxes of widgets a retailer receives each year and instantly know exactly what was inside and how many of them there were, without unpacking, handling, or manual scanning. A shelf wired with a reader would always know, in real time, what it held.

Second, the EPC can uniquely identify each individual item of merchandise rather than simply identifying a product line. Each tag can serve as a pointer to a particular database entry, with each database entry describing a *particular* television set, automobile transmission or can of beans.[25]

Starting in 2003, Wal-Mart and several other large retailers began pushing hard to implement RFID tagging in their supply chains on the case and pallet level. There was a strong case for implementing RFID here. The retailers urged that the ability to track cases and pallets wirelessly and automatically would give them a better picture of where manufactured items were in the supply chain and how fast it would take them to get there, enabling them to be more efficient in moving goods through the distribution process and making sure those goods were where they needed to be.[26] Retail industry analysts argued that 6–10% of spending on the supply chain was lost due to lack of visibility or poor visibility in the supply chain; RFID could address that.[27]

Wal-Mart, thus, directed its top hundred suppliers that, as of January 2005, it should be able to read RFID tags on each of the pallets and cases those suppliers ship to three Wal-Mart distribution centers. It planned to expand the program to a dozen distribution

[24] On the other hand, some barriers, particularly metal and fluid-rich substances such as the human body, may disrupt the radio signal. *See infra* notes 64–65 and accompanying text.

[25] These differences led one prominent senator to call RFIDs "barcodes on steroids." Senator Patrick Leahy, Remarks at The Dawn of Micro Monitoring: Its Promise and Its Challenges to Privacy and Security, Conference on "Video Surveillance: Legal and Technological Challenges," Georgetown University Law Center (Mar. 23, 2004), http://leahy.senate.gov/press/200403/032304.html.

[26] *FTC RFID Workshop, supra* note 20, at 13–14 (testimony of Sue Hutchinson, Product Manager, EPCGlobal).

[27] *Id.* at 52–53 (testimony of Britt Wood, Senior Vice President, Retail Indus. Leaders Ass'n), *available at* http://www.ftc.gov/bcp/workshops/rfid/wood.pdf.

centers and up to 600 stores by January 2006.[28] The move was evocative of Wal-Mart's leading role in causing suppliers to adopt old-fashioned bar codes in the mid-1980s.

The Wal-Mart project hit some snags. By January 2005, progress was slow. Suppliers were struggling with the technology; read rates were as low as 60%. Cooperating only because they were compelled to, suppliers were unwilling to spend more than a small fraction of the millions of dollars necessary to make the project work smoothly.[29] Thus, while more than one hundred suppliers were participating in Wal-Mart's pilot as of the start of 2005, fewer than half were tagging all of the pallets and cases they shipped to the three test distribution centers. Some suppliers put off tagging altogether while they completely overhauled their IT infrastructure; some were tagging as little as 2%.[30] By March 2006, Wal-Mart had managed to expand the program to three hundred suppliers, shipping products through five distribution centers[31]; it announced that by January 2007 it would increase participation to six hundred suppliers and additional distribution centers serving as many as a thousand stores.[32] While it met its thousand-store goal only a few months late, Wal-Mart has announced that it will delay installing readers in those distribution centers–so that the RFID-equipped cases and pallets at the distribution

[28] *FTC RFID Workshop*, *supra* note 20, at 120 (testimony of Simon Langford, Manager of RFID Strategy, Wal-Mart).

[29] *See* Barnaby J. Feder, *Despite Wal-Mart's Edict, Radio Tags Will Take Time*, N.Y. TIMES, Dec. 27, 2004, at C3, *available at* http://www.nytimes.com/2004/12/27/technology/27rfid.html?ex=1261803600&%2338;en=dc83fdfbd986e222&%2338;ei=5088&.

[30] *See id.*

[31] *See* Mel Duvall, *Wal-Mart's Faltering RFID Initiative*, BASELINE, Oct. 3, 2007, http://www.baselinemag.com/article2/0,1540,2191749,00.asp; Marc Songini, *Wal-Mart Details Its RFID Journey*, COMPUTERWORLD, Mar. 2, 2006, http://www.computerworld.com/industrytopics/retail/story/0,10801,109132,00.html. In RFID pilot stores, Wal-Mart has significantly reduced out-of-stocks and has been able to replenish empty shelves three times faster. *See also RFID Update from Wal-Mart*, IDTECHEX, Oct. 17, 2005, http://www.idtechex.com/products/en/articles/00000313.asp.

[32] *See RFID Update from Wal-Mart*, *supra* note 31; *see also* Jo Best, *Wal-Mart Demands Double RFID Chips with Groceries*, CNET NEWS.COM, Sept. 13, 2006, http://news.com.com/Wal-Mart+demands+double+RFID+chips+with+groceries/2100-1047_3-6115318.html.

center will be invisible to it.[33] Its suppliers have continued to be resistant.[34]

Around the time of the 2003 Wal-Mart announcement, several other major retailers—including Target and Albertson's in the United States,[35] and Tesco and Metro in Europe—announced similar plans.[36] None have been without difficulties. Target began a slow rollout in 2005, working with 100 suppliers.[37] Albertson's did the same (although a purchase of 5000 RFID readers, announced in 2006, suggested a plan to ramp up deployment).[38] European retailing giant Metro announced in 2004 an RFID rollout that, it planned, would by December 2005 include 100 suppliers, 269 stores, and eight distribution centers.[39] It did not go that quickly; by the summer of 2006, about forty of its suppliers were placing tags on pallets.[40] Metro

[33] *See* Marc L. Songini, *Wal-Mart Shifts RFID Plans*, COMPUTERWORLD, Feb. 26, 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=284115&intsrc=news_ts_head.

[34] *See* Evan Schuman, *The RFID Hype Effect*, EWEEK.COM, Feb. 27, 2006, http://www.eweek.com/article2/0,1895,1931978,00.asp.

[35] *FTC RFID Workshop*, *supra* note 20, at 224 (testimony of Chris Boone, Program Manager, IDC); Josh McHugh, *Attention, Shoppers: You Can Now Speed Straight through Checkout Lines!*, WIRED, July 2004, at 151, *available at* http://www.wired.com/wired/archive/12.07/shoppers.html. Other large retailers seemed ready to follow suit. *See* Jacqueline Emigh, *More Retailers Mull RFID Mandates*, EWEEK.COM, Aug. 19, 2004, http://www.eweek.com/article2/0,1759,1637597,00.asp ("all of the top 25 retailers have RFID initiatives either in place or under consideration").

[36] Wal-Mart's push, and the continuing buzz over RFID in the marketplace, caused a substantial number of corporate IT departments to begin or consider RFID pilots, even without any obvious way to get return on that investment; they feared they would be left behind if they did not.

[37] Laurie Sullivan, *Target and Suppliers Using RFID, Sources Say*, INFORMATIONWEEK, June 8, 2005, http://informationweek.com/story/showArticle.jhtml?articleID=164301344.

[38] *Wal-Mart to Buy 15k RFID Readers; Albertsons 5k*, RFID UPDATE, Apr. 18, 2006, http://www.rfidupdate.com/articles/index.php?id=1097.

[39] Jo Best, *Retailer to Follow RFID Test with Full Rollout*, ZDNET ASIA, Sept. 3, 2004, http://www.zdnetasia.com/news/hardware/0,39042972,39192342,00.htm.

[40] *Metro's Suppliers Face Deadline on Updated RFID Standard*, FOOD PRODUCTION DAILY, June 15, 2006, http://www.foodproductiondaily.com/news/ng.asp?id=68458-metro-rfid-epc; John Blau, *RFID on All Goods 15 Years Off, Says Retail Giant*, INFOWORLD, Mar. 8, 2006, http://www.infoworld.com/article/06/03/08/76222_HNrfidadoption_1.html?RADIO%20FREQUENCY%20IDENTIFICATION%20-%20RFID.

attributed a significant part of the delay to the rollout of an updated Gen2 version of the tag specifications and announced that it was looking towards beginning case-level tagging by the end of 2006; as of September 2006, though, it still had only 22 stores participating in its case-level tagging program.[41]

Case and pallet level tagging has so far not lived up to its advance publicity. Key to the deployment problem is the fact that the benefits of RFID tagging in this context accrue to retailers, but the costs are borne by suppliers.[42] This led to "slap and ship" tagging as suppliers made the minimum changes necessary to comply with Wal-Mart mandates, and other retailers held back to see whether Wal-Mart and other early adopters succeeded.[43] The pallet/case market, thus, was "the nearest thing to a black hole" in the RFID market in 2006; RFID hardware suppliers sold tags and readers at substantial losses, and consumer packaged goods companies did their best to avoid even those costs.[44] It seems clear by now that Wal-Mart's initial expectations for quick adoption were unrealistic.[45] Tagging in the

[41] Evan Schuman, *Metro Group Divorcing Grocery Scan from Payment*, EWEEK.COM, Sept. 13, 2006, http://www.eweek.com/article2/0,1895,2015462,00.asp. In Great Britain, supermarket chain Tesco announced ambitious plans in 2003 for case-and-pallet level RFID in its supply chain. *See* Jo Best, *Tesco Takes RFID into All Extra Superstores*, SILICON.COM, Sept. 30, 2004, http://networks.silicon.com/lans/0,39024663,39124558,00.htm. It ended up modifying those plans substantially. Struggling with too-long tag read times and restrictive EU spectrum-management regulation, *see RFID Update from Tesco*, IDTECHEX, Oct. 4, 2005, http://www.idtechex.com/products/en/articles/00000296.asp, it shifted away from placing disposable tags on shipping trays and pallets to a new plan locating permanent tags on the cages and trollies used to deliver goods from distribution centers to stores. *See* Andy McCue, *Tesco to Track Milk Deliveries by RFID*, CNET NEWS.COM, June 1, 2006, http://news.com.com/Tesco+to+track+milk+deliveries+by+RFID/2100-1033_3-6079022.html; Jonathan Collins, *Tesco Revises RFID Plans*, RFID J., Apr. 7, 2006, http://www.rfidjournal.com/article/articleview/2243.

[42] *See* Jonathan Katz, *Making RFID Work*, INDUSTRYWEEK, Feb. 1, 2006, http://www.industryweek.com/ReadArticle.aspx?ArticleID=11347. Another obstacle in Europe stemmed from restrictive spectrum-management rules. *See* Mark Roberti, *New ETSI RFID Rules Move Forward*, RFID J., Nov. 9, 2004, http://www.rfidjournal.com/article/articleview/1229/1/1; *RFID Update From Tesco*, *supra* note 41.

[43] Larry Dignan, *Suppliers Push Back at RFID Demands*, BASELINE, Aug. 31, 2005, http://www.findarticles.com/p/articles/mi_zdcis/is_200508/ai_n15325218/print; John R. Johnson, *The Case of the Missing Mandates*, DC VELOCITY, July 2005, http://www.dcvelocity.com/viewpoints/?article_id=559; Feder, *supra* note 29.

[44] Das, *supra* note 7.

[45] *See* Schuman, *supra* note 34.

inventory chain is a complex enterprise and lacks agreed-upon standards and sufficiently advanced software support. All of these problems are solvable with time, though, and industry analysts seem to agree that, in the end, RFID's benefits for the inventory process will make case-and-pallet deployment inevitable.[46]

What about other uses for RFID? The initial buzz over RFID in the inventory process was not limited to the case and pallet level. A variety of companies engaged in *item-level* testing of tags on a broad range of consumer goods; that is, their trials involved the placement of RFID tags on individual consumer items. Gillette (which announced in early 2003 that it would purchase 500 million RFID tags)[47] worked with retailers to test "smart shelves," as an adjunct to item-level tagging, for inventory control. With a reader on each shelf and a tag on each package of razor blades, it reasoned, the data proprietor would always know how many packages were on the shelves, without having to count them. Benetton made plans early to put RFID in individual items of clothing, but pulled back after a publicity firestorm; consumers expressed alarm about the prospect of walking around with their shirts speaking silently and wirelessly to networked computing devices in their paths.[48]

Other companies were less deterred. Marks & Spencer conducted initial trials of item-level RFID tags in menswear, and more recently, trials in connection with other items, including women's underwear; it appears committed to testing item-level RFID as a stock control system.[49] Levi's conducted a small pilot in which certain of its men's jeans sold at a single (undisclosed) U.S. store carried external RFID hang tags.[50] Gap and Abercrombie also conducted small pilots.[51]

[46] *See id.*

[47] David M. Ewalt, *Gillette Orders 500 Million RFID Tags*, INFORMATIONWEEK, Jan. 6, 2003, http://www.informationweek.com/story/IWK20030106S0007.

[48] *Benetton Explains RFID Privacy Flap*, RFID J., June 23, 2003, http://www.rfidjournal.com/article/view/471/1/1.

[49] *FTC RFID Workshop*, *supra* note 20, at 265–68 (testimony of James Stafford, Head of RFID, Marks & Spencer); Bert Moore, *RFID: Invading Women's Underwear?*, AIM GLOBAL, Mar. 9, 2006, http://www.aimglobal.org/members/news/templates/template.aspx?articleid=841&zoneid=24. Marks & Spencer also deployed three and a half million RFID tags on its returnable food trays, which cycle between the store and its food suppliers. *FTC RFID Workshop*, *supra* note 20, at 263–64.

[50] Press Release, CASPIAN, Spychipped Levi's Brand Jeans Hit the U.S. (Apr. 27, 2006), *available at* http://www.spychips.com/press-releases/levis-secret-testing.html.

Yet few of these pilots seem to be going anywhere. Neither Gap nor Abercrombie, their pilots over and done with, seem to be investing in RFID tagging.[52] Gillette is focusing its own current efforts on investigating the tagging of cases, pallets, and promotional displays, not individual items.[53] While some new trials are taking place,[54] they do not seem to add up to a robust trend favoring increased item-level roll-out.[55]

There was reason, as far back as 2004, to doubt the business case for item-level tagging. To begin with, it was not clear whether the cost of RFID tags would drop sufficiently. It is hard to imagine widespread distribution of item-level tags unless the price per tag drops below five cents and harder to imagine tags on really cheap consumer items—say, boxes of cereal and bars of soap—unless the price per tag drops to below a penny.[56] But the cost of even the least expensive tag in 2004 was more than ten cents by some accounts and forty cents by others.[57] As one analyst explained the problem:

[51] *See* Jonathan Collins, *RFID Implementation is an Art*, RFID J., June 14, 2006, http://www.rfidjournal.com/article/articleview/2427/1/1.

[52] *See id.*

[53] *See* Mary Catherine O'Connor, *Gillette Fuses RFID with Product Launch*, RFID J., Mar. 27, 2006, http://www.rfidjournal.com/article/articleprint/2222/-1/1.

[54] *See, e.g.*, Marc Songini, *Dutch Bookseller Unveils Item-Level RFID System*, COMPUTERWORLD, Apr. 25, 2006, http://www.computerworld.com/printthis/2006/0,4814,110858,00.html.

[55] *But see* LOGICACMG & GS1, EUROPEAN PASSIVE RFID MARKET SIZING 2007–2022, at 2 (Feb. 2007), http://www.logicacmg.com/file/7468 (urging that "RFID is still poised for significant growth in Europe" with most of that growth in the short term coming from item-level tagging of high-value items).

[56] *Progress with Item-Level RFID Special Report*, THE IDTECH WEB J., Feb. 2004, at 5, *available at* http://www.idtechex.com/pdfs/en/L6931K9077.pdf [hereinafter *Progress with Item-Level RFID Special Report*]. (To make a tag for less than a penny, you would want to print RFID circuits and memory on conventional multi-station printing presses, along with the regular product packaging, using layers of conductive and non-conductive inks. There are now signs of movement in that direction but it is still a long way away.); *see* Raghu Das, *Chipless RFID-The End Game*, IDTECHEX, Feb. 20, 2006, http://www.idtechex.com/products/en/articles/00000435.asp.

[57] *See* ALLEN FRIEDMAN, PREDICTIONS AMID THE HYPE: ASSESSING THE RISKS OF RETAIL RFID AND PRIVACY 7–8 (2004), http://www.sccs.swarthmore.edu/users/02/allan/RFID_Privacy_Hype.doc; *see also FTC RFID Workshop*, *supra* note 20, at 57 (testimony of Britt Wood, Senior Vice President, Retail Industry Leaders Association) (estimating a cost of twenty to forty cents per tag).

> The first challenge is cost reduction, the damned things cost too much. And the next three or four iterations of Moore's Law on this is going to be cost reduction. And then the next problem is that they still cost too much, because the antennas cost too much. And beyond that, there's a real problem in getting the chip-antenna bonding to work right . . . as you make these chips smaller and smaller and you try to attach them to the antenna . . . [Y]ou know what happens when it's hard to attach these things? They cost too much.[58]

The cost numbers have been recalcitrant. As one company's CIO put it more recently: "The costs of tags are 40 cents, and it is 10 cents to put them on. But we're not getting a 50 cent return. If we're lucky, we get 7 cents."[59]

It is possible that tag costs may yet come down substantially. Not too long ago, an Israeli company announced that it would sell tags in volumes of 100 million or more for as little as five cents. It sidestepped questions of whether the offer was, in essence, a loss leader.[60] Even with inexpensive tags, though, taking advantage of item-level tagging will require retailers to incur the costs of purchasing and installing reader networks, training reader operators, and putting in place back-end data systems to manage the information. Some observers estimate that hardware costs for RFID will amount to only 3% of the total with software to process the huge amounts of data generated by the network making up 75%.[61] The hardware and software costs associated with large-scale implementation of systems such as smart shelves, which feature large numbers of readers and terabytes of data per day, may be prohibitive.[62]

[58] *FTC RFID Workshop*, *supra* note 20, at 249 (testimony of Jim Waldo, Sun Microsystems).

[59] Larry Dignan, *Suppliers Push Back at RFID Demands*, BASELINE, Aug. 31, 2005, http://www.baselinemag.com/print_article2/0,1217,a=159259,00.asp.

[60] Mark Roberti, *SmartCode Offers 5-Cent EPC Tags*, RFID J., May 1, 2006, www.rfidjournal.com/article/articleview/2296.

[61] *See FTC RFID Workshop*, *supra* note 20, at 57–58 (testimony of Britt Wood, Senior Vice President, Retail Industry Leaders Association); *see also* Danny Bradbury, *Extending the Enterprise: RFID: It's No Supply Chain Saviour -Not Yet Anyway*, SILICON.COM, Sept. 8, 2004, http://www.silicon.com/research/specialreports/enterprise/0,3800003425,39123656,00.htm.

[62] *See FTC RFID Workshop*, *supra* note 20, at 250 (testimony of Jim Waldo, Sun Microsystems).

Item-level RFID is desirable for inventory control only to the extent it can generate useful information more quickly and cheaply than can currently available technologies such as bar-code scanning.[63] If item-level tagging is to justify its costs, it will have to be markedly more convenient and more reliable than lower-tech approaches. But there is room for doubt on that score, at least when it comes to low-value items. Early adopters wrestled with the fact that RFID tags are subject to considerable interference from items in the retail environment, such as fluids and metal,[64] not to mention nylon conveyor belts and dense materials like frozen meat and chicken parts.[65] Even in environments that could be optimized for RFID, such as distribution centers receiving arriving pallets, readers were sometimes unable to read more than 80% of the tags.[66] In the words of one industry analyst: "Every site's a little different. You can't just throw up antennae; there's a tuning aspect. This is dirty fingernail stuff."[67] It is more difficult still to get satisfactory read rates for RFID

[63] For an excellent early analysis of RFID costs, concluding that "the economic benefits of item-level tagging appear to be exaggerated or hyped by proponents of RFID technology," *see* FRIEDMAN, *supra* note 57, at 9–15. For a similar thought from another angle, here is a poll question reproduced from Frontline magazine:

> One of the first areas of RFID adoption in the supply chain will be at the pallet or unit-load level. Based on your own operations, where on the unit load would it make the most sense to place the RFID tag?
>
> - On the pallet or conveyance itself.
> - On the stretch wrap.
> - On the last carton on the pallet.
> - On my application for unemployment when our RFID project goes over budget

available at http://www.clearorbit.com/files/FrontlineSolutionsVoltek.pdf (the poll question is in the right hand margin of the document).

[64] *Progress with Item-Level RFID Special Report, supra* note 56, at 7. Other frequency bands, moreover, present their own problems. *Id.*

[65] *See* David Margulius, *The Rush to RFID,* INFOWORLD, Apr. 9, 2004, at 38, *available at* http://www.infoworld.com/pdf/special_report/2004/15SRrfid.pdf; *see also* FRIEDMAN, *supra* note 57, at 6–7.

[66] Margulius, *supra* note 65, at 38.

[67] *Id.* (quoting Tig Gilliam, partner, IBM Business Consulting Services). In David Freeman Hawke's *Nuts and Bolts of the Past: A History of American Technology, 1776-1860* (1988), the "men with dirty fingernails" were inventors and mechanics at home on the shop floor, going from one machine to the next, comfortable with tightening enough bolts here and replacing enough gears there to make their inventions work. So too here.

tags on the retail store floor, which cannot be optimized for RFID readers the way a distribution center can.[68] While current reports indicate better read rates with tags conforming to the new Gen2 specification, the problem is still substantial.

All this suggests that there are major obstacles in the way of the industry's dream of "put[ting] a radio frequency ID tag on everything that moves in the North American supply chain."[69] Some executives predict that we will see mass adoption of RFID on the item level, but not until the 2020s or later.[70] With a time frame twenty years or more in the future, though, no prediction is reliable.

What about other uses of RFID? Manufacturers and service providers have chosen to deploy RFID in a wide range of more specialized applications. Michelin, for example, began fleet testing RFID in tires in 2003. Each tire's unique identification number, in EPC format, is associated in an external database with the Vehicle Identification Number ("VIN") of the car on which it is mounted, and with information describing when and where the tire was made, its maximum inflation pressure, its size, and so on.[71] The tags are too expensive for passenger-car use, but are in production now for airplanes and fleet trucks.[72] Tire-industry engineers are developing

[68] *See* ROSS STAPLETON-GRAY, SCANNING THE HORIZON: A SKEPTICAL VIEW OF RFIDS ON THE SHELVES (2003), http://www.stapleton-gray.com/papers/sk-20031113.pdf. Stapleton-Gray also notes disadvantages of RFID for retailers in terms of competitive marketing considerations and vulnerability to corporate espionage and counterfeit tags. At the very least, these concerns may push retailers towards closed systems and away from the relatively open Object Name Space.

[69] Lori Valigra, *SmartTags: Shopping Will Never be the Same*, CHRISTIAN SCI. MONITOR, Mar. 29, 2001 (quoting Steven Van Fleet, program director, International Paper), quoted in Katherine Albrecht, *Supermarket Cards: The Tip of the Retail Surveillance Iceberg*, 79 DENV. U.L. REV. 534, 561 n.163 (2002).

[70] *See* Blau, *supra* note 40; *see also FTC RFID Workshop*, *supra* note 20, at 60 (testimony of Britt Wood, Retail Industry Leaders Association, stating that significant item-level tagging is unlikely within the next ten years); *id.* at 59 (suggesting that it will be 2017 before we see item-level tagging on products cheaper than ten dollars); *id.* at 109 ("the economics behind item-level just don't make sense right now for retailers to implement.").

[71] *See* John Johnson, *Where the Rubber Meets the Road*, DC VELOCITY, May 2006, http://www.dcvelocity.com/viewpoints/?article_id=215; Laurie Sullivan, *Michelin Expands RFID Tests*, INFORMATIONWEEK, Oct. 12, 2004, http://www.informationweek.com/shared/printableArticle.jhtml?articleID=49901180; *Michelin Introduces Radio Frequency Tire Identification Technology*, MOTOR TREND, Jan. 16, 2003, http://www.motortrend.com/features/news/112_news011603_tire.

[72] *See* Johnson, *supra* note 71.

specifications to combine that functionality with sensors monitoring temperature and pressure.[73]

A variety of automobile manufacturers incorporate RFID into the ignition key, so that the key can identify itself to the anti-theft system.[74] So far, indeed, transportation-related uses—also including cards and tickets for busses and trains—have accounted for more than 40% of the 2.4 billion RFID tags that one source estimates have been sold to date.[75]

RFID tags have been extensively deployed in library books, raising concerns about tracking and surveilling individuals via their First Amendment activity.[76] They are used to track livestock and pets: more than 50 million pets have RFID tags.[77] Indeed, any technology that keeps track of pets works for children as well; schools have used RFID-equipped identification badges, schoolbooks and clothing to track elementary and middle school students.[78]

Access cards, and other uses relating to financial, security, and safety applications, account for another 25–30% of tags sold to date. Banks have issued tens of millions of RFID-equipped credit cards; you can find RFID credit-card readers in CVS pharmacies, McDonald's restaurants and some movie theaters.[79] The advantage of RFID here is

[73] *See* Sullivan, *supra* note 71.

[74] *See FTC RFID Workshop*, *supra* note 20, at 16–17 (testimony of Dr. Daniel Engels, Executive and Research Director, Auto-ID Labs) (Ford); *Id.* at 68 (testimony of William Allen, Marketing Communications Manager, Texas Instruments RFID Systems) (Jeep, Chrysler, Mitsubishi, Toyota, Lexus).

[75] *See* RAGHU DAS & DR. PETER HARROP, RFID FORECASTS, PLAYERS & OPPORTUNITIES 2006–2016, at 20, http://www.idtechex.com/pdfs/en/P1637T1931.pdf.

[76] *See* Alorie Gilbert, *RFID, Coming to a Library Near You*, CNET NEWS.COM, Oct. 18, 2004, http://news.com.com/RFID,+coming+to+a+library+near+you/2100-1012_3-5411657.html.

[77] Cathy Booth-Thomas, *The See-It-All Chip*, TIME, Sept. 14, 2003, http://www.time.com/time/globalbusiness/article/0,9171,1101030922-485764,00.html.

[78] *See* Nicole A. Ozer, *Rights "Chipped" Away: RFID and Identification Documents* (Jan. 2007), *available at* http://stlr.stanford.edu/2007/01/rfid_technology.html; Jo Best, *Japan Schoolkids to be Tagged with RFID Chips*, ZDNET NEWS, July 12, 2004, http://www.zdnetasia.com/news/hardware/0,39042972,39186467,00.htm.

[79] *See* John Schwartz, *Researchers See Privacy Perils in No-Swipe Credit Cards*, N.Y. TIMES, Oct. 23, 2006, at C1, *available at* http://www.nytimes.com/2006/10/23/business/23card.html?ei=5070&en=d51440266e3f7c33&ex=1173844800; JIMMY ATKINSON, CONTACTLESS CREDIT CARDS CONSUMER REPORT 2006 (2006), *available at* http://www.findcreditcards.org/reports/contactlessreport.pdf.

that the user need not swipe her card through a reader; it is sufficient to bring it into the reader's general vicinity. The danger, of course, is that unauthorized readers may be able to pull information from the card as well.[80]

It is possible to imagine a whole lot of uses for a technology in which objects can be uniquely identified without direct contact. If you wanted the milk in your refrigerator to notify you (or your supermarket) if you failed to drink it by its pull date, RFID technology would be a good way to go.[81] Indeed, you could tie a slightly more elaborate tag to a nanosensor that checked for spoilage directly.[82]

In the "Way Cool" department, Mattel has introduced a collectible card game called Hyperscan in which the cards bear RFID tags; players, after swiping the cards over the base unit, compete against each other in onscreen games in which their avatars wield the cards they have just swiped. After the battle, the base unit writes new information to the tags on the winner's cards, to make them more powerful in the next battle.[83]

A recent summary from RFID consultant (and evangelist) IDTechEx illustrates the breadth of current and potential uses:

[80] It appears, indeed, that data security architecture on many credit cards today is surprisingly bad. *See* Schwartz, *supra* note 79.

[81] *Compare* Vint Cerf, Growing Up in a Digital World, Address Given at the Global Internet Summit 2000 (Aug. 7, 2000), http://www.govtech.com/gt/2191 (imagining the Internet-equipped refrigerator, but assuming that one would manually scan a milk carton's bar code when putting it in the fridge), *with* John C. Dvorak, *Smart Homes, Dumb Ideas*, PC MAG., June 26, 2000, http://www.shed.com/digests/digests2000/06-30-00.txt.

[82] *See* Jack Uldrich, *Now You See It. . .*, ADVANTAGE, Feb. 2004, (describing use of nanotechnology to detect milk spoilage).

[83] Seth Schiesel, *It's a Game, It's a Toy, It's Mattel's Big Gamble*, N.Y. TIMES, July 20, 2006, at E1. A list of actual or proposed uses for RFID, indeed, could go on at some length. A plan to keep tabs on the elderly envisions placing RFID tags on objects in the subjects' homes, and networked readers on their persons, to keep track of their handling the tagged items. *See* Mark Baard, *RFID Keeps Track of Seniors*, WIRED, Mar. 19, 2004, http://www.wired.com/news/medtech/0,1286,62723,00.html. Casinos have put RFID tags in chips to block counterfeiting, identify stolen chips, and track gamblers' play. An Italian manufacturer introduced a washing machine equipped to read RFID washing instruction tags in clothing. *See Merloni Unveils RFID Appliances*, RFID J., Apr. 4, 2003, http://www.rfidjournal.com/article/articleview/369/1/1/. A German supermarket, for a brief time, inserted RFID tags in supermarket loyalty cards–which gave the store the capability, while someone carrying the loyalty card was in the store, to pull up his entire buying history without his being aware that the query was taking place and without any other basis for the store's knowing who he was. It abandoned the experiment after consumer outcry.

> RFID is monitoring the post in Algeria and Bosnia-Herzegovina and is being used in the Philippines in the form of Stored Value Cards to replace cash and reduce queues. Road tolling is a use in Slovakia. For proof of ownership it is on reindeer in Lapland. In precious wild plants in New Zealand, it has led to arrests under conservation orders. RFID tags on prepared sushi meals in Japan permit the staff to automate payment and stocktaking but in Antarctica it has enabled research on the behaviour of penguins. In Thailand, they like to put RFID on chickens for disease control and they use it in cock fighting. In South Africa, RFID tracks ore but in Turkey they encounter it as a loyalty card.
>
> In Canada, they have been tracking food trolleys in their aircraft but Italy has RFID on intelligent mooring buoys in marinas giving personalised promotional messages when you tie up. Australia tags boats for theft prevention. The Australians tag racehorses by law but the Canadians tag fish for conservation. In the UK RFID has been used to research the behaviour of insects including butterflies and IDTechEx has several studies of the tagging of elk but not in China, where pandas are the centre of attention.
>
> RFID is the basis of an automated tour of a museum in Korea and it prevents theft in art galleries in France - an improvement on the crude performance of the traditional anti-theft tag in shops and libraries, which is not RFID. [Implementations range f]rom casino chips in the USA to a multifunctional bank card in Azerbaijan, national identification cards in Estonia, China and Oman, weapons permits in Honduras, laptop theft prevention in Brazil and police evidence bags in the UK . . . .[84]

There has been a move underway for some time in the pharmaceutical industry to tag shipments of drugs to pharmacies with unique serial numbers on RFID tags. That unique identifier could tie each package to its complete manufacturing and dispensing history, as a guarantee that the drug was what its package held it out to be and

[84] Dr. Peter Harrop, *RFID Exotica*, IDTECHEX, Nov. 13, 2006, http://www.idtechex.com/products/en/articles/00000499.asp.

was being sold in authorized channels.[85] This move was driven heavily by federal and state requirements that medications have a chain-of-custody pedigree showing, from the time a medication left the factory, which entity held it, for how long, and who the entity passed it to. RFID initially was seen as a natural way (though not the only way) for drug manufacturers to achieve good chain-of-custody pedigrees. Recently, though, the FDA has noted substantial obstacles to the use of RFID to identify medication packages, including concerns about privacy, the security of confidential business transaction data, the accuracy and speed of RFID reader systems, and the effect of RFID on sensitive products.[86] Only a small number of high-value and heavily counterfeited medications, such as Viagra, are likely to see extensive RFID tagging in the near future.[87]

One of the most eye-catching proposed uses for RFID relates to implanting tags into people subcutaneously. A Spanish nightclub, two years ago, went ahead and injected RFID tags into some of its customers, who thereby got free access to the club's VIP area.[88] As the club owner explained: "You won't have to carry a wallet. By simply passing by our reader, the Baja Beach Club will know who you are and what your credit balance is."[89] Mexico's attorney general, about the same time, announced that he and 160 members of his staff had been equipped with chips implanted in their arms, to authenticate their access to secure office areas and to enable them to be found

[85] *See* U.S. FDA, COMBATING COUNTERFEIT DRUGS: A REPORT OF THE FOOD AND DRUG ADMINISTRATION § D.1.e (Feb. 2004), *available at* http://www.fda.gov/oc/ initiatives/counterfeit/report02_04.html#radiofrequency.

[86] *See* U.S. FDA, FDA COUNTERFEIT DRUG TASK FORCE REPORT: 2006 UPDATE § IV.B (2006), *available at* http://www.fda.gov/oc/initiatives/ counterfeit/report6_06.html.

[87] *See US Legislation Slows Pharma RFID Tracking*, CXOTODAY.COM, Feb. 8, 2006, http://www.cxotoday.com/cxo/jsp/article.jsp?article_id=71218&cat_id=911.

[88] *See* Press Release, Infowars, Applications Continue to Grow for Applied Digital Solutions' VeriPay: Baja Beach Club in Barcelona, Spain Employs RFID Technology for Cashless Payment System (Apr. 5, 2004), *available at* http://www.infowars.com/print/bb/ bajaimplantupdate.htm.

[89] The Spanish-language text ("No hace falta llevar monedero. Con sólo pasar por nuestro lector, Baja Beach Club conocerá quién es, y de qué saldo dispone.") no longer appears on the club's website. Another copy of the Spanish text, and an English translation, can be found at http://www.infowars.com/print/bb/bajaimplant.htm. While not all content on the Infowars site is reliable, the translation appears accurate.

"anywhere inside Mexico" in the event of assault or kidnapping.[90] This was, well, silly, and more than a little curious; how a chip with a read range of a few inches would allow the wearer to be found anywhere in the country was left unexplained.[91]

More recently, the Food and Drug Administration ("FDA") approved the implantation into human subjects of RFID tags referencing the subjects' medical records.[92] According to the manufacturer, about sixty people so far have agreed to be chipped.[93] A Cincinnati company implanted chips in two workers to test the use of implanted chips for secure-area access.[94]

It is hard to read about chipping live human beings with equanimity. Yet actual instances of human implantation have been unserious, isolated, or hypothetical.[95] We can expect tremendous market resistance to any initiative calling for the implantation of RFID tags in live people.

Indeed, RFID deployment to date presents something of a paradox. On the one hand, RFID is in many ways a tremendously powerful enabling technology, with a wide range of potential applications (many

[90] *See Mexican Officials Get Chipped*, WIRED, July 13, 2004, http://www.wired.com/news/technology/0,1282,64194,00.html; Press Release, CASPIAN, Mexican Government Promotes Myth of RFID Security (July 19, 2004), http://spychips.com/press-releases/mexican-implants.html; Monica Campbell, *Law Enforcement in Mexico Goes a Bit Bionic*, CHRISTIAN SCI. MONITOR, Aug. 4, 2004, http://www.csmonitor.com/2004/0804/p01s04-woam.html.

[91] The manufacturer's Mexican distributor had earlier announced plans to implant RFID tags in children as an anti-kidnapping device; searchers would place readers in "strategic locations where a search is being conducted," as well as malls, bus stations, and similar locations. *See* Julia Scheeres, *Tracking Junior with a Microchip*, WIRED, Oct. 10, 2003, http://www.wired.com/news/technology/0,1282,60771,00.html.

[92] Barnaby J. Feder & Tom Zeller, Jr., *Identity Chip Planted Under Skin Approved for Use in Health Care*, N.Y. TIMES, Oct. 14, 2004, http://www.nytimes.com/2004/10/14/technology/14implant.html.

[93] Press Release, Spychips.com, RFID Implants: Fine for Thee, But Not for Me (Dec. 7, 2005), http://www.spychips.com/press-releases/verichip-thompson-no-implant.html.

[94] Associated Press, *A First in U.S.: Chipped Beef*, WIRED, Feb. 14, 2006, http://www.wired.com/news/technology/0,70217-0.html.

[95] I include in this category the Verichip Corporation's lobbying for mandatory chips in the bodies of foreign guest workers, to be used "at the border . . . [and] for enforcement purposes at the employer level." Fox & Friends interview with Scott Silverman, Chairman of the Board of VeriChip Corporation (May 16, 2006), *available at* http://www.spychips.com/press-releases/silverman-foxnews.html.

of them, like livestock tagging, presenting no interesting privacy issues). On the other hand, in the United States at least, the highest-volume applications have not yet generated a business case suggesting the sort of return on investment that would make the project worthwhile. This is most notably true in the context of inventory control. Focus on RFID hardware—on tags and readers—has led to a heavily populated hardware supplier sector, in which suppliers, bleeding cash, do their best to differentiate themselves, while prospective buyers are holding back, unconvinced that RFID can actually make money for them.[96] The complexity and costliness of deployment, as well as the entrenched nature of existing bar-code-based tracking systems, have left many firms unenthusiastic about adopting the technology.[97]

If we step away from current technology and short-term business models, we may get a different view of the technology's potential. Looking far to the future, author Bruce Sterling has argued that RFIDs are the forerunners of profound, irreversible technological transformation, comparable to the Industrial Revolution in both social upheaval and the technological advances it will bring.[98] Sterling foresees a world shot through with RFIDs and networked sensors, all generating information, all leaving information trails and microhistories of the objects to which they are attached. That sort of information, he continues, will be necessary if society is to know enough about itself, and to exert enough control over its physical circumstances, to survive.[99] The society of the future, he urges, will rely on having detailed digital representations of objects and their environments, enabled and enriched by the information these sensors bring, in order for its members to better understand it, to design it, and to design for it (in part through effortless fabrication from digital models).[100]

[96] Sandra Gittlen, *The Failure of RFID*, COMPUTERWORLD, June 15, 2006, http://cwflyris.computerworld.com/t/601111/1423078/22956/0.

[97] John S. Webster, *Forecast 2006: RFID*, COMPUTERWORLD, Jan. 2, 2006, http://www.computerworld.com/managementtopics/management/story/0,10801,107308,00.html?source=NLT_EB&nid=107308.

[98] *See* STERLING, *supra* note 1, at 8–14, 85–94.

[99] *See id.* at 45–47, 97–101.

[100] *See id.* at 102–05.

The transformation, he acknowledges, will have downsides. "In engaging with a technology so entirely friendly toward surveillance, spying, privacy invasion and ruthless technical intrusion on previously unsoiled social spaces, we are playing with fire."[101] But, he continues, we do not banish fire from society because of its dangers; rather than engaging in "fatalistic handwringing" when it comes to "technology's grim externalities and potentials for deliberate abuse," the answer lies in "design thinking and design action."[102] I have a variety of difficulties with Sterling's vision, all best left to a paper other than this one, but my objections do not detract from his basic point that networked sensors can provide incredibly important information, and provide the basis for technological innovation—and RFIDs, in important ways, are just a special case of networked sensors.

III. RFID AND GOVERNMENT IDENTITY DOCUMENTS

One enthusiastic and growing RFID market is the government. Governments are not constrained by the need for adequate return on investment and not all of the issues slowing down business take-up are relevant in the government context. Section Three of this article explores government deployment of RFID technology. After a brief overview, it first discusses, and criticizes, the government's initiative to embed RFID in passports. It then examines the Department of Homeland Security's efforts to incorporate RFID technology into two sets of travel documents: the PASS travel document for people traveling between the U.S. and Canada and the I-94 that all temporary visitors to the U.S. must carry. It concludes by describing initiatives to embed RFID in a variety of other government identification documents.

To date, thirteen agencies of the U.S. government have implemented, or plan to implement, a specific RFID deployment plan.[103] Some of those straightforwardly relate to logistics support,

[101] *Id.* at 12–13.

[102] *Id.* at 13.

[103] GAO, INFORMATION SECURITY: RADIO FREQUENCY IDENTIFICATION IN THE FEDERAL GOVERNMENT (2005), *available at* http://www.gao.gov/new.items/d05551.pdf. In response to a GAO questionnaire, only one of the thirteen agencies answered that it believed there were legal issues associated with RFID use, and only six responded that they were concerned with security issues.

tracking the movement of shipments or other materials.[104] Others are less innocuous from a privacy perspective: the Department of Health and Human Services ("HHS") and the Treasury Department plan to use RFID for physical access control, and the Department of Transportation for "screening." The State Department has already begun issuing passports equipped with RFID, and the Department of Homeland Security intends to use RFID-equipped documents for border control. The General Services Administration ("GSA") is procuring government ID cards that identify themselves wirelessly[105] (although GSA, alert to the public-relations implications of its labels, insists that because these contactless cards encrypt communications from tag to reader, they are not RFID).[106]

An initial key adopter of RFID for the logistics chain was the U.S. Department of Defense ("DoD"), which announced in 2004 that it would require all suppliers by January 2005 to put passive RFID tags on "the lowest possible part, case or pallet packaging."[107] Full-scale deployment is now underway; DoD expects all 26 of its Defense Distribution Centers to be ready to accept RFID-tagged product by the end of 2007.[108]

The State Department has moved successfully to embed RFID in passports. The United States was closely involved in the formulation of an International Civil Aviation Organization committee recommendation that all passports and other travel documents store electronic data on "contactless integrated circuit" chips (which is to say, RFID technology or a close relation).[109] The U.S. government

[104] The U.S. General Services Administration mandates for the use of RFID to help it manage information on the buildings, fleets of cars, and other products it oversees; *see* Sun Microsystems, RFID Streamlines Processes, Saves Tax Dollars, http://www.sun.com/br/government_1216/feature_rfid.html (last visited Jan. 17, 2007).

[105] *See* GAO, *supra* note 103, at 13–14.

[106] *See* sources cited *supra* note 17 and accompanying text.

[107] That is, suppliers should put tags on individual parts whenever possible; when item-level tagging is impossible, they may tag cases instead; when they can do neither of those, they may place tags on pallets. Matthew French, *For DOD Logistics, Tags are It!*, FED. COMPUTER WEEK, Nov. 2, 2003, http://www.fcw.com/print/9_40/news/81316-1.html.

[108] John Johnson, *DOD Suppliers Will Start Tagging Product Soon*, DC VELOCITY, June 7, 2006, http://www.dcvelocity.com/articles/rfidww/rfidww20060607/rfid_dod.cfm; Mary Catherine O'Connor, *DOD Grants ODIN $14.6 Million Contract*, RFID J., May 25, 2006, http://www.rfidjournal.com/article/articleview/2368.

[109] *See* INT'L CIVIL AVIATION ORG., BIOMETRIC TECHNOLOGY ON MACHINE READABLE TRAVEL DOCUMENTS–THE ICAO BLUEPRINT (2003), http://www.icao.int/icao/en/atb/fal/fal12/

then moved quickly to implement that recommendation.[110] New U.S. passports now have RFID embedded.[111] The passport electronically stores the bearer's picture and the other information physically printed on the passport.[112] In response to pressure, the State Department has incorporated some important privacy protections in its technology. The passport cover incorporates shielding, so that the digital material cannot be read when the cover is closed. Further, the digital information on the passport is encrypted; the key is printed on the passport and is gained by swiping the passport through an optical reader.[113] Thus, the attacker is not supposed to be able to pull unencrypted data from the card without physical access to it.

It is useful, from a security standpoint, to have encrypted digital information on a passport: it makes it harder to forge passports or to use stolen ones. It is another matter altogether, though, to make the digital information on a passport available wirelessly. Notwithstanding significant efforts on the State Department's part to achieve a secure design for an RFID-enabled passport, there appear to be significant security shortcomings in its passport design. For one thing, the printed key is simply a combination of the passport number, date of birth, and expiration date. If an attacker can learn or brute-force that information, it can read—perhaps clone—the passport data.[114] Moreover, the technology presents the risk that information

documentation/fal12wp004_en.pdf; *see also* Letter from Privacy International et al., to the International Civil Aviation Organization (Mar. 30, 2004), http://www.privacyinternational.org/issues/terrorism/rpt/icaoletter.pdf.

[110] Time to Get a New USA Passport, http://hasbrouck.org/blog/archives/000433.html (Oct. 14, 2004, 10:27 PST); Wilson P. Dizard III, *Smart Passport Field Narrows to Four*, GOV'T COMPUTER NEWS, Oct. 12, 2004, http://gcn.com/vol1_no1/daily-updates/27620-1.html.

[111] Bruce Schneier, *Fatal Flaw Weakens RFID Passports*, WIRED, Nov. 3, 2005, http://www.wired.com/news/privacy/0,1848,69453,00.html. Other countries have taken similar steps. Japan, for example, has begun issuing RFID-enabled passports and will dispense more than 3.55 million in the next year. Jonathan Collins, *Japan Issues E-Passports*, RFID J., Mar. 28, 2006, http://www1.rfidjournal.com/article/view/2224.

[112] *See* Frank E. Moss, Deputy Assistant Sec'y for Passport Servs., U.S. Dep't of State, Remarks to the Information Technology Association of America 4–5 (Mar. 28, 2006), *available at* http://www.itaa.org/es/Frank%20Moss%20Remarks.pdf.

[113] Schneier, *supra* note 111.

[114] Steve Boggan, *Cracked It!*, THE GUARDIAN, Nov. 17, 2006, http://www.guardian.co.uk/idcards/story/0,,1950226,00.html; RFID enabled e-passport skimming proof of concept code released, e-mail from Adam Laurie to the Bugtraq mailing list (Oct. 27, 2006, 17:35:43) *available at* http://lists.openwall.net/bugtraq/2006/10/27/24.

broadcast by an open passport (potentially readable, even without specialized equipment, as much as ten feet away and perhaps farther[115]), even though encrypted, can still be used as a persistent unique identifier of the person carrying it.[116] That is, attackers may be able to associate with each passport a string of data that is unique to it and consistent over time; an attacker could use that information to track the passport holder.[117] The State Department has introduced a randomized unique ID feature that the agency says will mitigate this attack, but it makes no claim that the feature will eliminate it.[118]

The Department of Homeland Security is seeking to issue travel documents that will present a different set of privacy and security issues. DHS has sought to incorporate RFID technology into two distinct sets of travel documents. The first is the PASS travel document for people traveling by land between the U.S. and Canada. A recently enacted U.S. law requires citizens to have passports to enter this country from Canada, Mexico, or the Caribbean; because it costs a citizen nearly a hundred dollars to get a passport, the PASS card was conceived as a cheaper alternative.[119]

DHS's current plans are to incorporate a 96-digit unique serial number into each card, using EPC Gen2 technology essentially

[115] The standard read range associated with the ISO 14443 chips used in passports is about four inches, but in practice read ranges can be greater; the State Department has conceded as much as ten feet in practice. *See* Bruce Stewart, *Digging in to RFID*, O'REILLY, Mar. 9, 2006, http://www.oreillynet.com/conferences/blog/2006/03/digging_in_to_rfid.html. *See also* Moss, *supra* note 112 (reporting laboratory readers as far away as "a few feet"). Others have claimed a read range of up to 69 feet, but it is not established that those observers were using the ISO 14443 chip. NIST has reported readings of an ISO 14443 chip at thirty feet. *See* Stewart, *supra* note 115.

[116] Schneier, *supra* note 111. Activist Bill Scannell, in part for this reason, has referred to RFID-equipped passports as "terrorist beacons." E-mail from Bill Scannell, disseminated by David Farber on the IP list (Mar. 28, 2005), *available at* http://www.interesting-people.org/archives/interesting-people/200503/msg00245.html.

[117] *See infra* text following note 151; *see also*, RFID Passports at CFP, http://hasbrouck.org/blog/archives/000558.html (Apr. 17, 2005, 12:30 PST) (quoting Bruce Schneier's prediction that your unique passport ID number "will be sold to Choicepoint for a dollar and added to your file the first time it is read").

[118] *See* Moss, *supra* note 112, at 6; Press Release, Media Note, U.S. Dept. of State, Department of State Begins Issuing Electronic Passports to the Public (Aug. 14, 2006), http://www.state.gov/r/pa/prs/ps/2006/70433.htm.

[119] *See Amendment Would Delay New U.S. Travel Card*, CARD TECH., May 26, 2006, http://www.cardtechnology.com/article.html?id=20060526I5ECSJNY.

identical to that used on retail inventory control cards.[120] The serial number, thus, would likely be broadcast promiscuously and could be read under the right circumstances as far away as 25 to 40 feet, even if the card itself were not displayed. The card would not incorporate passport security features. The Department contemplates that travelers approaching the border will remove their PASS cards from their protective sleeves and place them on their car dashboards. About 30 feet before the border kiosk, they will pass under a portal containing a card reader; the reader will extract the PASS card IDs and display the associated information on a computer screen for the border control official.[121]

This is problematic from a privacy and security standpoint. It would not be difficult for third parties to pick up and track the unique ID on the card.[122] Without access to the DHS database, the attacker could not learn the personal information associated with the card, but they would easily be able to use the card's output as a persistent unique identifier. Indeed, having done so, they could use that information to clone the card–to program an inventory-control tag so that it looks, electronically, like somebody else's PASS card. At that point, it would be relatively easy to forge a PASS card for anybody who looked somewhat like the target, and all of the electronic traces it would leave would be the target's.[123]

The Department of Homeland Security also planned to embrace RFID in connection with I-94s, the documents that all nonimmigrants

[120] A public comment period relating to those plans ended on January 8, 2007. DHS has not yet announced what actions it is taking in light of the comments it has received.

[121] *See* Press Release, Dep't of Homeland Sec., DHS Proposes to Expand the Use of Vicinity RFID in Implementing Western Hemisphere Travel Initiative (Oct. 17, 2006), http://www.dhs.gov/xnews/releases/pr_1161114866740.shtm; Smart Card Alliance Identity Council, *Western Hemisphere Travel Initiative PASS Card: Recommendations for Using Secure Contactless Technology vs. RFID,* SMART CARD ALLIANCE, June 2006, http://www.smartcardalliance.org/alliance_activities/whti.cfm; Michael Arnone, *Beaming Across the Border: DHS and State Disagree on Which Security Technology to Use for Border Protection,* FCW.COM, Apr. 24, 2006, http://www.fcw.com/article94156-04-24-06-Print.

[122] While DHS plans to mitigate this threat by issuing travelers a plastic sleeve for their card, travelers may not replace their cards in the sleeves promptly and some will surely lose the sleeves altogether. *See* Smart Card Alliance Identity Council, *supra* note 121; Letter from American Electronics Association et al., to Frank E. Moss, Deputy Assistant Sec'y, U.S. Dep't of State, and Elaine Dezenski, Acting Assistant Sec'y, Border and Transp. Sec. Policy, U.S. Dep't of State (Jan. 30, 2006), *available at* http://www.aeanet.org/GovernmentAffairs/imVxLuTyjJJAdCYpdTbUqO.pdf#search=%22ruid%20epassport%22.

[123] *See* sources cited *supra* note 114.

(that is, noncitizens admitted into the U.S. other than for permanent residence) must carry at all times. Congress has directed that the agency use I-94s to match up nonimmigrants' entry records with their exit records; the problem is that while DHS creates and maintains records when nonimmigrants *enter* the country, it has no similar records created when they *leave*. Accordingly, the agency does not know which nonimmigrants are in the country at any given time.

The Department of Homeland Security initially concluded that the answer to this identification gap was for every visitor to carry, at all times, an I-94 equipped with an RFID chip similar to that contemplated for the PASS card. The chip would contain a unique serial number pointing to a database entry created at the border, containing the traveler's biographic and biometric information. The document would broadcast that unique serial number, promiscuously, via RFID; DHS could read the tags at U.S. exit points without the participation of the person carrying the document.[124] The serial number could be read each time the visitor came within range of a reader, whether DHS's or anyone else's. In the Department's words, this would allow it to compile a "complete travel history" for each visitor.[125] DHS had a pilot program in place at five U.S. border ports doing just that.

The program was the subject of vigorous criticism. As one critic put the point, "this is the first case in which anyone in the USA (even non-citizens), other than convicted criminals or those subject to specific restrictive court orders issued following adversary and evidentiary legal proceedings, will have been required by law to carry remote radio tracking devices."[126] Privacy advocates urged that the RFID tag serial number would both serve as a persistent unique identifier and identify the carrier to anyone with an RFID reader as a nonimmigrant visitor.[127] At the same time, technology experts (perhaps providing some reassurance to the privacy advocates)

[124] *See id.*; Letter from Electronic Frontier Foundation et al., to Chief Legal Counsel, Office of Passport Policy Planning and Advisory Servs. (Apr. 4, 2005), *available at* http://www.epic.org/privacy/rfid/rfid_passports-0405.pdf#search=%22passport%20%22contact%20technology%22%22.

[125] Update on RFID Passports and Traveller Tracking, http://www.hasbrouck.org/blog/archives/000735.html (Aug. 19, 2005, 14:29 PST) (quoting DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT UPDATE FOR THE US-VISIT PROGRAM, at 14).

[126] *Id.*

[127] *See* Letter from Electronic Frontier Foundation et al., *supra* note 124.

questioned whether agency RFID devices would be able to read the tag information on a sufficiently reliable basis.[128]

DHS now appears to have abandoned this project.[129] Read rates in the pilot program were abysmal; at one test site, RFID readers correctly identified only 14% of vehicles carrying a person holding an RFID-enabled I-94.[130] Moreover, it became clear that, to avoid disabling signal interference, each site would need individually designed equipment and infrastructure, to take into account each site's individual "physical configuration of buildings, roadways, roofs, gantries, poles and other surfaces against which the signals can bounce."[131] And because the program contemplated no *biometric* examination of departing visitors (nor was any feasible, given current resource and technological constraints), even perfectly working RFID technology could confirm only that the I-94 document was leaving the country; it could not confirm that the person to whom the document had been issued was along for the ride.[132]

A variety of other United States government RFID initiatives are in the works. The Transportation Security Agency and Coast Guard are planning a Transportation Worker Identification Credential program, under which various workers in the transportation industry will be required to apply for and receive RFID-enabled identification cards.[133]

[128] *See* Stewart, *supra* note 115. One RFID vendor, reacting to agency specs calling for 100% read rates on tags inside vehicles as much as 25 feet away moving as fast as 55 mph, had commented: "Yeah, and I think they believe in Tinker Bell, too." Evan Schuman, *U.S. Homeland Security Delays RFID Plan*, EWEEK.COM, Feb. 28, 2006, http://www.eweek.com/article2/0,1895,1931979,00.asp.

[129] *See Chertoff: RFID Program to Be Abandoned*, UPI, Feb. 9, 2007, http://www.upi.com/NewsTrack/Top_News/2007/02/09/chertoff_rfid_program_to_be_abandoned/7815.

[130] GAO Testimony Before the Subcomm. on Terrorism, Tech., and Homeland Sec. of the S. Judiciary Comm., U.S. Senate: Border Security: US-VISIT Program Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry, GAO-07-378T, at 18 (Jan. 31, 2007), http://www.gao.gov/new.items/d07378t.pdf.

[131] *Id.* at 18–19.

[132] *Id.* at 19.

[133] *See* Press Release, Dep't of Homeland Sec., Fact Sheet: Transportation Worker Identification Credential (TWIC) Prototype (Nov. 17, 2004), http://www.dhs.gov/xnews/releases/press_release_0558.shtm; Press Release, Dep't of Homeland Sec., DHS Implements Immediate Measures to Secure Access to Ports (Apr. 25, 2006), http://www.dhs.gov/xnews/releases/press_release_0893.shtm; Letter from Randy Vanderhoof, Executive Director of the Smart Card Alliance, to members and friends of the

GSA is planning an RFID-enabled Personal Identity Verification card for federal employees and contractors.[134] DHS is looking at an RFID-enabled First Responder Authentication Card for use in emergency response coordination efforts among first responder categories within federal, state, and local agencies.[135] All of these would comply with a technology standard for Personal Identity Verification of Federal Employees and Contractors (FIPS 201) promulgated by NIST.[136]

Yet even as State Department, GSA, and DHS plans for incorporating RFID into identity documents have gone forward, we are seeing some backlash in this country against other comparable government implementations. Two years ago, the state of Virginia was exploring proposals for RFID-equipped driver licenses.[137] A year ago, many analysts believed that DHS would mandate RFID for all driver licenses under its REAL ID Act[138] authority.[139] The political landscape, however, has now changed. State agencies have examined RFID in the context of their driver license programs and found it unsuited to their needs.[140] DHS's just-issued REAL ID rulemaking proposal rejects RFID for driver licenses, writing that "there is not an

Alliance (May 2006), http://www.smartcardalliance.org/newsletter/may_2006/ letter_0506.html.

[134] *See* NIST.gov, About Personal Identity Verification (PIV) of Federal Employees and Contracts, http://csrc.nist.gov/piv-program/index.html (last visited Jan. 17, 2008) [hereinafter *About Personal Verification Project*].

[135] *See* Letter from Randy Vanderhoof, *supra* note 133.

[136] *See About Personal Identity Verification Project*, *supra* note 134; *see also* SMART CARD ALLIANCE, *supra* note 17.

[137] Mark Baard, *RFID Driver's Licenses Debated,* WIRED, Oct. 6, 2004, http://www.wired.com/news/privacy/0,1848,65243,00.html.

[138] REAL ID Act of 2005, Pub. L. No. 109-13, tit. II §§ 201–207, 119 Stat. 231, 311–16 (2005).

[139] *See, e.g.*, Posting of Bruce Schneier to Schneier on Security, Real ID, http://www.schneier.com/blog/archives/2005/05/real_id.html (May 9, 2005, 09:06 PST).

[140] *See* Thomas A. Schatz, *Chip-Based Driver's Licenses Pose Enormous Problems*, CIO, Feb. 2, 2006, http://www.cio.com/blog_view.html?CID=17416. More recently, a house of the California legislature voted preemptively to ban RFID in driver licenses. *See* Marisa Torrieri, *California RFID Bill Holds as Senator Considers Industry Concerns*, INT'L BIOMETRIC INDUS. ASS'N, Feb. 1, 2006, http://www.ibia.org/biometrics/ industrynews_view.asp?id=384; *see also* Anne Broache, *Tech Industry Attacks State Anti-RFID Laws*, CNET NEWS.COM, Apr. 19, 2006, http://news.com.com/Tech+industry+ attacks+state+anti-RFID+laws/2100-1028_3-6062985.html.

identifiable need for driver's licenses and identification cards to be routinely read from a distance." It provides instead that driver licenses must include information digitally encoded into a 2-D bar code.[141] Analysts have described this as an about-face prompted by increasing public concern over the security, privacy, and monetary implications of DHS's original plans.[142] As of this writing, two states have voted not to comply with the REAL ID Act and similar bills have so far passed one chamber of the legislatures of eight other states.[143]

In sum, the U.S. government's current record on deploying RFID technology is mixed. RFID is now part of U.S. passports; as I will explain in section VI, use of RFID technology there is undesirable and ill-considered. DHS is pushing ahead to incorporate RFID into its PASS cards, in an even more problematic move, and GSA is moving to build the technology into a variety of government IDs. On the other hand, our government is seeing some resistance. DHS has recognized the technology's unsuitability for I-94s and has recognized its political unacceptability (at least for now) in driver licenses.

All this, however, is only part of the picture: the United States is not the only country planning RFID initiatives.[144] In the People's

[141] Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed. Reg. 10,820, 10,837 (proposed Mar. 9, 2007) (to be codified at 6 C.F.R. pt. 37), *available at* http://www.dhs.gov/xlibrary/assets/nprm_realid.pdf at 75–76. The document discusses the possibility that state driver licenses incorporating RFID could serve as PASS (border crossing) cards. *Id.* at 10,841–42, *available at* http://www.dhs.gov/xlibrary/assets/nprm_realid.pdf at 92–94; *see* sources cited *supra* notes 119–23 and accompanying text.

[142] Renee Boucher Ferguson, *DHS Issues Proposed Regulations for Real ID Act*, EWEEK.COM, Mar. 2, 2007, http://www.eweek.com/article2/0,1895,2100036,00.asp.

[143] *See* Real Nightmare, Status of Anti-Real ID Legislation in the States, http://www.realnightmare.org/news/105 (last visited Jan. 17, 2008).

[144] Some time ago, both the European and Japanese central banks discussed incorporating RFID tags in currency. *See* John Leyden, *Japan Yens for RFID Chips*, THE REGISTER, July 30, 2003, http://www.theregister.co.uk/2003/07/30/japan_yens_for_rfid_chips; Kim Yong-Young, *Radio ID Chips May Track Banknotes*, CNET NEWS.COM, May 22, 2003, http://www.news.com/2100-1017_3-1009155.html; Junko Yoshida, *Euro Bank Notes to Embed RFID Chips by 2005*, EE TIMES, Dec. 19, 2001, http://www.eetimes.com/story/OEG20011219S0016; *but see* Mark Roberti, *The Money Trail*, RFID J., Aug. 4, 2003, http://www.rfidjournal.com/article/articleview/523/1/2 (such reports were "wildly premature"). The U.S. government is said to have expressed interest as well. *See* Sun Microsystems, Inc., RFID Streamlines Processes, Saves Tax Dollars, http://www.sun.com/br/government_1216/feature_rfid.html (last visited Jan. 17, 2008). The nominal goal here was to make counterfeiting more difficult, as well as perhaps keeping track of money laundering and black-market transactions. Some reports indicated that tags for currency would have a read range of only a few millimeters, so that information seekers could

Republic of China, the government is issuing more than 1.3 billion RFID "resident identification" cards, directly storing—and broadcasting—personal identifying information including the holders' names and birth dates.[145] A subset of those cards, as many as 150 million in the short term, will incorporate information relating to work history, educational background, religion, ethnicity, police record, medical insurance status, landlord's phone number, and personal reproductive history (for enforcement of the "one child" policy).[146] The cards will not be able to be read from as great a distance as DHS's; it appears that the tags' reliable range will be in the neighborhood of a foot. But the fact that the entire population, apparently, will be required to carry the RFID-equipped card, identifying themselves wirelessly, without demand, is an order of magnitude beyond anywhere DHS has gone so far.[147]

IV. ANALYZING RFID THREATS

It is hard to predict the future. Many RFID implementations are still on the drawing board; we do not yet know which ones will actually be rolled out. Tags may become entirely commonplace in connection with some application I have not discussed in this

not identify currency from a distance, but details were hard to come by; the tag generally discussed in this connection was Hitachi's μ-chip, which is said to have a read range of about a foot. *See Hitachi Unveils Smallest RFID Chip*, RFID J., Mar. 14, 2003, http://www.rfidjournal.com/article/view/337/1/1. On privacy issues associated with RFID in currency, *see* ARI JUELS & RAVIKANTH PAPPU, SQUEALING EUROS: PRIVACY PROTECTION IN RFID-ENABLED BANKNOTES (2003), *available at* http://www.rsa.com/rsalabs/staff/bios /ajuels/publications/euro/Euro.pdf.

[145] *See* Sumner Lemon, *China to Issue 1.3 Billion RFID Identification Cards*, INFOWORLD, Mar. 9, 2006, http://www.infoworld.com/article/06/03/09/76259_HNchinarfidcards_1.html; *see also* Ning Xiao, *RFID in China*, IDTECHEX, Aug. 30, 2006, http://www.idtechex.com/products/en/articles/00000491.asp; *National ID Project Moves China to Head of the Pack in Radio Frequency Technology*, CARDTECHNOLOGY, Feb. 21, 2007, http://www.cardtechnology.com/article.html?id=20070221PGYABPF5.

[146] *See* Keith Bradsher, *China Enacting a High-Tech Plan to Track People*, N.Y. TIMES, Aug. 12, 2007, http://www.nytimes.com/2007/08/12/business/worldbusiness/ 12security.html?ei=5088&en=df3f7b36de098b00&ex=1344571200.

[147] Like U.S. passports, the tags will broadcast their holders' identifying information directly, rather than just displaying a serial number pointing to a database entry. It is not immediately clear what level of access control the card technology will support, and thus the extent to which the information will be available to anyone with a reader, rather than just authorized government agents.

article.[148] It may be that all the barriers to item-level tagging of retail goods will be overcome in the next fifteen years.

A few years ago, many of us paying attention to RFID were most interested in commercial applications. Privacy scholars know the importance of commercial privacy threats, given the industry's huge ability and incentive to monetize information about potential purchasers. Moreover, it was hard to ignore the science-fictional flair of the notion of one's underwear broadcasting one's identity. But commercial businesses will implement privacy-invasive (or any other) technologies only to the extent they see return on investment. Further, at least some commercial businesses are sensitive to public concerns about RFID technology; no business can afford to be entirely indifferent to those concerns. All this has somewhat restrained the short-term commercial RFID privacy threat.

Government, by contrast, has different incentives and no market constraints. Because government budgets are limited, even a government agency has an incentive to accomplish tasks using less-expensive technologies rather than more-expensive ones. But if government decision-makers decide that a particular technology is desirable, they can deploy it even where industry would see no return on investment. And not all government entities are equally sensitive to public privacy concerns. In contrast to the State Department, which has tried to grapple with those concerns in good faith, DHS has seemed less interested in treating privacy (and public perceptions of privacy) as a high priority.

In this article, I will continue on the assumption that RFID technology will ultimately become widespread, although not necessarily pervasive, in some facets of everyday life–whether government, commercial, or both. We need to consider, thus, how we should think about that from a privacy standpoint.

This section of the article describes the characteristics of RFID that generate privacy concerns. It goes on to describe three different categories of RFID implementation that can present privacy threats: first, one in which an RFID device makes available the holder's personal identifying information; second, one in which the RFID device provides a pointer to a limited-access database containing the holder's personal identifying information; and third, one in which the RFID device does not make available personally identifying information (directly or through pointers to a database). For each category, this article evaluates the extent to which use of the RFID

[148] *See infra* note 205.

technology presents one of three related categories of threat, which I call surveillance, profiling, and action. The article pays specific attention to the issues presented by inventory control tags, which as an initial matter fall into the third category. There is reason to question, though, whether the third category is robust: linking persistent identifiers to personally identifying information may turn out to be quite easy. Finally, this section of the article addresses the significance of cryptographic access control as a means of addressing RFID threats.

What specific characteristics of RFID give rise to privacy concerns? First, RFID-equipped goods and documents may reveal information about themselves, and hence about the people carrying them, wirelessly, to people whom the subjects might not have chosen to inform. If an ordinary citizen is carrying items or documents equipped with passive RFID tags, then complete strangers can read information from those tags without any current or prior relationship with the person carrying them, indeed without having known anything about that person at all before cranking up the tag reader. The subject need not be aware that the information is being collected.

Second, that capability follows the target through space and reveals to data collectors how the target moves through space. RFID presents new privacy concerns in part because it allows observers to learn something about a target that most other privacy-invasive technologies do not—and that is *where* the subject is physically. It is thus, quite directly, a surveillance technology. Finally, not only does the profile that RFID technology helps construct information about where the subject is and has been, but also RFID signifiers travel *with* the subject in the physical world, conveying information to devices that otherwise would not recognize it, and that can take actions based on that information.

In evaluating these threats, it is important to distinguish among different sorts of RFID implementations. We can start with an RFID device that directly stores, and makes available to anyone with a reader, the holders' personal identifying information. This would be the category that the People's Republic of China resident identification card described earlier would fall into, if it were adopted without significant access controls preventing non-government actors from reading the cards.[149]

[149] The American Association of Motor Vehicle Administrators standard for state driver licenses requires that data digitally encoded onto a driver license be unencrypted. *See* Minimum Standards for Driver's Licenses, *supra* note 141, at 10,838. If a state chose to implement RFID in connection with a AAMVA-compliant driver license, that information too

This is the most obviously privacy-invasive scenario. Data on the RFID tag can be read either by the entity responsible for the target carrying the RFID tag, or by an unrelated (and unauthorized) third party, and either way the person carrying the tag may not be aware of the privacy invasion. The twenty-meter read range I referred to earlier as a theoretical maximum for inexpensive passive tags leaves room for substantial surveillance capabilities. Other tag implementations have shorter read ranges, but readers can effectively invade privacy even with shorter read ranges. One can embed an RFID reader, invisibly, in floor tiles, carpeting, or a doorway.[150] A read range of only a few feet is entirely adequate to track people coming through a door. So the opportunities for surveillance are extensive.

This set of RFID implementations presents three related privacy threats. The first is geographic surveillance. Any person with access to a reader will know the identity of each person carrying a tag (and in the PRC example just noted, all residents would be required to carry one by law). The ability to read names off RFID tags, given that RFID situates its data subjects in space, means that every reader network is a Panopticon geolocator. A listener seeking to compile a database with the identities of nearly all of the people attending an event in a building would merely have to station readers at the building entrance. The rest of the data collection and analysis would be automatic.

The second threat is profiling. The data collector can maintain a profile on the target and include in that profile not only the results of the surveillance, but also any other information gleaned at a distance from the tag. In the case of a passport, this would include identifying numbers, address, and physical characteristics. (Recall that the data collector may be a third party, not the government entity that created the tag in the first place.)

The third is the one Ravi Pappu describes as the "action threat."[151] After learning a person's identity via RFID, people or devices associated with the reader network can take actions regarding that person (ranging from further surveillance and arrest on the one hand, to displaying targeted ads on the other) based on their knowledge of who the subject is and what it is like.

could be transmitted in the clear. It seems unlikely, though, that a state would make such a choice in today's political environment.

[150] CASPIAN ET AL., *supra* note 11, at 2.

[151] RAVI PAPPU, THINGMAGIC, LLC, PRESENTATION AT THE RFID PRIVACY CONFERENCE: PRIVACY AND SECURITY IN THE EPC NETWORK 11 (Nov. 15, 2003), *available at* http://www.rfidprivacy.us/2003/papers/pappu.pdf.

Next, let us consider an implementation in which RFID tags, while providing no significant access control, do not broadcast personal identifying information directly. Rather, they merely broadcast pointers to entries in a limited-access database containing the holders' personal identifying information. DHS's proposed PASS card is an example of such an implementation. How does that change the privacy calculus?

It does not change the calculus at all, of course, when it comes to privacy threats from the entity responsible for the tag and in control of the database. A U.S. citizen carrying a PASS card (at least so long as the card is out of its protective sleeve), is still subject to surveillance, profiling, and action threats from DHS, and from any other entity that has obtained database access from DHS. A key question, thus, in evaluating the nature of the privacy threat in such an implementation, is the extent to which third parties can buy, barter, or otherwise gain access to the database to which the tag points. To the extent that governmental security-related information sharing is extensive today, privacy threats associated with DHS RFID are accordingly greater.

To the extent that a third party cannot gain access to the database, an important privacy-related concern remains: the data on the tag can serve as a persistent unique identifier of the person carrying it. Without knowing anything about the *meaning* of the serial number on a particular tag, a person with a reader can use that serial number to aggregate data about a particular subject over time—if only on the level of "this is the same guy who was here making trouble last week." The person carrying the tag is still subject to the surveillance, profiling, and action threats, except that those threats will be directed at the nameless (for now) holder of the particular unique tag, not at the subject as a named person. Moreover, if the link between the tag number and the subject's identity makes its way later into an information broker's database, the privacy threats become identical to those posed in our first scenario. I will return to that point later in this discussion.

What if an RFID tag neither points to, nor carries, personal identifying information? An item-level retail inventory control tag, after all, does not contain the name or address of the person carrying it; it merely points to a database entry revealing that it is, for example, a sweater from a particular manufacturer, of a particular style and color, with a given unique serial number. Where are the privacy threats there?

To answer that question, it is useful to know at the outset the extent to which third parties will know the meaning of those tag serial numbers. Assume that an item-level inventory control tag conforms to the EPCGlobal architecture. The system contemplated by the Auto-ID

Center as a standard for RFID use in the retail supply chain, establishing the Object Name Space ("ONS") as a distributed database, is well-designed for easy and transparent access to tag data, by actors up and down the supply chain, in the name of increased supply-chain visibility and coordination. Initially, it appeared that the system might be quite open. More recently, though, it has come to seem likely that manufacturers will restrict access to portions of the ONS under their own control, or avoid the ONS entirely, so that RFID scanning will not reveal sensitive competitive information.[152] If a manufacturer restricts access to portions of the ONS under its own control, then the distributed database might inform the casual requester that the Electronic Product Code ("EPC") on a particular tag referenced a product made by shoe-manufacturer Mephisto, but that the rest of the information referenced by the EPC was stored in a limited-access database on Mephisto's servers. This will ameliorate some of the privacy threat.

One should not take this point too far, though: the meaning of common tag object classes, identifying the type and model of goods supplied by a given manufacturer, may not stay secret long. Different manufacturers' policies will vary; and as manufacturers embrace the modern reality that they can monetize consumer information by selling it to aggregators, it is by no means clear that the information associated with tag data will remain closely held. It is at least possible, therefore, that a tag on the shoe you purchase in the future will tell anyone who asks, as you walk around town, that it is a Mephisto shoe style 17, size 9, in black, serial # 139421386. In that way, a wide range of strangers to you could learn, automatically and without direct contact, the data on the tags you are wearing or carrying, and could construct a snapshot profile of you.

That adds a new facet to the profiling threat. When I presented the profiling threat earlier, it was fairly straightforward: a data collector could enter in a profile, say, a person's address, lifted from his driver's license or resident identification card. Item-level tags on retail goods make this threat more interesting. Consumers might find themselves carrying a variety of different tags on different occasions. Profiling might incorporate data signaled by all of those tags—not (only) on identification documents, but on clothing, vehicles, and portable possessions. When an entity reads new information about the target from a different tag or tags, it could add to the profile associated with

[152] *See* STAPLETON-GRAY, *supra* note 68; *FTC RFID Workshop*, *supra* note 20, at 38 (testimony of Sue Hutchinson, Product Manager, EPCGlobal); *id.* at 222–23 (testimony of Christopher Boone, Program Manager, IDC).

that name any new characteristics associated with that new RFID information (as well as the unique tag numbers themselves).

One might object that this is not much of a privacy threat because information that readers will collect (such as the target's shoe style) will likely be visible to the naked eye in any event. Yet RFID is important from a privacy standpoint even where it only facilitates the collection of information that could otherwise be collected by analog means, by allowing for the automation of the information collection and storage process.[153] Imagine, after all, the movement of automobiles down a highway. There is nothing stopping a government from posting an employee to copy down license plate numbers or a camera to photograph them. That information, though, comes into being in analog format; it would be time-consuming and expensive to enter it into a digital database. As a result, the information will not in fact be entered digitally except on particular occasions when it is important and cost-effective to do so. By contrast, if a reader were positioned in the highway collecting data from RFID tags in automobile tires (with the tag data linked to automobile VINs in a separate database), then the collection of the data and its inclusion in a searchable digital database would be fully automated, cheap, and easy to do. RFID readers, in short, automate their information collection and collect the information in a format that makes its inclusion in networked databases trivial. That is important, because the cheaper it is to collect, store, and analyze information, the more information will in fact be collected, stored, and analyzed.[154]

If RFID use becomes widespread, then various commercial and governmental users are likely to deploy a wide range of discrete reader networks. If there are economic and political incentives for the proprietors of those various networks to share information (and there are likely to be), then we will face the functional equivalent of a single very large network. It will not matter if no particular set of readers is pervasive.[155]

[153] *See* Jeffrey Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 27, 29 (1995) ("If we direct our privacy-protection efforts at reinforcing our doors and curtains, we may miss the way in which modern means of information collection threaten our privacy by gathering up the pieces of our public lives and making them visible from a single point.").

[154] I owe this articulation to Lee Tien.

[155] Moreover, "[i]t does not take a ubiquitous reader network to track objects or the people associated with them. For example, automobiles traveling up and down Interstate 95 can be

It is useful here to draw one last distinction. It has already become clear from this discussion that while strangers can collect RFID data from tags on goods or documents in my possession, that data is not *necessarily* linked to my name or other personally identifying information.[156] In some situations giving rise to information privacy concerns, sensitive information is born already attached to the data subject's name or other personally identifying information. Think, say, of the information on driver licenses or passports, or credit-card purchase information.

In some situations, thus, a data collector will draw a link between my name (or other personally identifying information) and data on at least one RFID tag I carry. If I go into the Gap and buy a tagged sweater, then the Gap can link the sweater's EPC with my name and other information in its database. Assuming that the tag is not disabled at the point of sale or after, then every time I walk into the Gap wearing that sweater, store personnel will be able to know who I am without having to ask. If the Gap sells or trades the data linking my tag information with my personally identifiable information, then wherever I go *anyone* in possession of that data can read my tag and accordingly know who I am, and my profile, without having to ask.[157] In other situations, by contrast, RFID tag information, while attached to the geographic location or the physical person of the target, will not necessarily be attached to anyone's name or personally identifying information. The data collector may know what type of sweater I wear, but still may not know my name.

Where a target's tags themselves broadcast personally identifying information or can be linked to such information, the target is subject to a robust form of the profiling threat. A reader network can cheaply

tracked without placing RFID readers every few feet. They need only be positioned at the entrance and exit ramps." CASPIAN ET AL., *supra* note 11, at 6.

[156] In another context, pseudonymous payment schemes seek to protect privacy by attacking that link, decoupling purchase information from the buyer's identity. *See* Jonathan Weinberg, *Hardware-Based ID, Rights Management, and Trusted Systems*, 52 STAN. L. REV. 1251, 1279–80 (2000).

[157] The problem is reminiscent of that posed by a firm's linking computer users' cookie data with their offline identities. At the time of the Abacus-Doubleclick merger in 1999, the combined company announced plans to cross-reference Abacus's database of consumer buying habits—containing real names and addresses and detailed buying information—with Doubleclick's database of consumer Internet surfing and buying habits. It backed off in the face of Federal Trade Commission and state investigations, private lawsuits, and a consumer boycott. *See id.* at 1270. The analogy is imperfect, though, since consumers can avoid or delete cookies with rather more ease than they may be able to avoid or disable RFID tags.

and seamlessly collect RFID information from the target's belongings and documents, and easily add it to its profile. When an entity reads information from the subject's tags, it will be able to add to the profile associated with its name any new characteristics associated with that RFID information (as well as the unique tag numbers themselves). The target is also subject to a strong form of the surveillance threat, since the devices attached to the reader network will know who the person carrying the tags is. Finally, the target is subject to an equally strong form of the action threat.

Thus, for example, if my automobile windshield tag broadcasts a unique ID corresponding to my account in the university parking system, and that ID can be linked to my name, then any reader network with access to that link will know where my car is (or at least when it last came within range of a reader). The network can add that information about my travels to my profile, together with information derived from other RFID tags that appear in the same constellation, although the software may need to do some work to figure the likelihood that a particular tag is associated with some other person traveling in my car. And the network can notify police, say, if they have reason to want to talk to me when my car appears at particular locations, so that they can have the conversation they want.

By contrast, where a target's tags do not themselves broadcast personally identifying information (directly or through pointers to a database the reader has access to), then a stranger who knows nothing about the target other than what it can pull from its tags will not necessarily be able to make a connection between the target's RFID data and its name or other personally identifying information. This largely eliminates the profiling and surveillance threats: if a stranger reads my parking tag number but does not know which number is whose, he will not know that this is *my* car.

The target is still subject to a version of the action threat, though. Even without knowing the target's name, the listener can associate information with the target's physical being in a particular location, and take action based on that association–displaying particular advertisements to the target, steering it to particular goods the seller thinks may be of interest, offering the target differential rates, imposing obstacles to its admission to a mall.[158] If my tag information indicates that I wear a Rolex, a reader may not need to know my name in order to decide to treat me differently. Further, the tag number can

[158] *See* Kang & Cuff, *supra* note 12, at 106–07.

serve as a unique and semi-persistent identifier.[159] Anyone with an RFID reader situated near a place I go can collect information over time about me (the individual, located intermittently or long-term in a particular geographic space, who is associated with particular unique tag numbers). This information collection over time can inform the actions I have just described. And once those dossiers exist, they may be linked to my name at a later point.

Are these really separate scenarios? As profiling accelerates in the modern world, aided by the automatic, networked collection of information through technologies like RFID, information compiled by one data collector likely will increasingly be available to others as well; the economic (and homeland security) forces pushing in that direction are powerful. As a result, information linking tag data to my personal identity may well move easily into the hands of actors who are strangers to me in any meaningful sense.[160] Linking persistent identifiers to personally identifying information may turn out to be quite easy. As John Gilmore has put the point, the fact that an RFID payment tag provides persistent ID but does not broadcast the identity of its carrier is only privacy-protective "once,"

> until anyone who wants to correlates that token ID "blob" with your photo on the security camera, your license plate number (and the RFIDs in each of your Michelin tires), the other RFIDs you're carrying, your mobile phone number, the driver's license they asked you to show, the shipping address of the thing you just bought, and the big database on the Internet where Equifax will turn a token ID into an SSN (or vice verse) for 3c [sic] in bulk.[161]

That suggests that the privacy provided by tags (such as DHS's PASS card) that broadcast only serial numbers pointing to database entries is elusive; it may be all too easy for outsiders, such as information brokers to link the unique serial number with the target's identity sometime after its profile is created.

[159] I will describe them here as semi-persistent, since, after all, if a tag is attached to a retail good I am carrying, I may end up carrying or wearing the good only some of the time.

[160] This suggests, though, that data privacy restrictions aimed at preventing the collection, or sharing, of information linking tag data to personally identifying information may be one way to limit privacy threats. *See infra* Section VI.

[161] Posting of John Gilmore to Financial Cryptography, https://financialcryptography.com/mt/archives/000552.html (Sept. 20, 2005, 10:29 EST).

There is one more important set of RFID implementations for us to consider. So far, I have discusses RFID implementations that promiscuously broadcast tag data to third parties. That is not an inherent characteristic of RFID technology. One can manufacture RFID tags with sophisticated access controls, which will not release their information unless the reader established through a cryptographic handshake that the tags' programmer had authorized it.[162] That technology is expensive, however, for a tag securely to authenticate an authorized reader via public key cryptography is well beyond the resources of the sort of low cost tag used in inventory control applications.[163] Nonetheless, if one is willing to pay for more expensive tags, one can supplement cryptography with other technical protections aimed at the ability of RFID tags to supply globally unique identity. More sophisticated RFID architecture allows tags to emit not a single, unchanging, unique ID, but a series of random pseudonyms, which can only be understood by authorized verifiers.[164]

There has been no movement by device manufacturers or standards bodies to incorporate these approaches into ordinary inventory-control tags and one would hardly expect there to be. The business case for RFID in the retail supply chain depends on keeping the tags inexpensive, yet firms can make RFID tags cheap only by making them dumb. In order for a tag to implement access controls, it needs to add logic gates, and that increases its size and cost. A manufacturer cannot make a passive tag smart enough to handle, say, public-key encryption, without completely blowing the business case for the foreseeable future. So run-of-the-mine inexpensive passive tags, and in particular those currently intended for use in the retail supply chain, do not incorporate access controls, and disclose their data promiscuously to anybody with a reader.

[162] *See* SANJAY E. SARMA ET AL., RFID SYSTEMS, SECURITY & PRIVACY IMPLICATIONS § 4.4 (2002), *available at* http://www.autoidlabs.org/uploads/media/MIT-AUTOID-WH-014.pdf; *see also* ISTVAN VAJDA & LEVENTE BUTTYAN, LIGHTWEIGHT AUTHENTICATION PROTOCOLS FOR LOW-COST RFID TAGS (2003), *available at* http://www.vs.inf.ethz.ch/ events/ubicomp2003sec/papers/secubi03_p01.pdf.

[163] SARMA ET AL., *supra* note 162, § 4.3.

[164] *See* U.S. Patent Application No. 20040222878 (filed Nov. 11, 2004), *available at* http://appft1.uspto.gov/netahtml/PTO/search-adv.html (search for "20040222878" and follow the hyperlink for the application titled "Low-complexity cryptographic techniques for use with radio frequency identification devices"); *see also* MIYAKO OHKUBO ET AL., CRYPTOGRAPHIC APPROACH TO "PRIVACY-FRIENDLY" TAGS (2003), *available at* http://www.rfidprivacy.us/ 2003/papers/ohkubo.pdf (changing tag data through a randomized hash chain).

But some cards are more sophisticated. The Personal Identity Verification card mentioned earlier, planned for identifying federal employees and contractors, as well as the Transportation Worker Identification Credential issued in prototype by the Transportation Security Administration and the First Responder Authentication Card being issued in DHS pilots will all use RFID chips meeting ISO 14443 smartcard specifications.[165] Those cards incorporate more sophisticated access control, designed to deny third parties the opportunity to read the data on the cards. Do they ameliorate the privacy threats discussed above?

It is surely the case that less availability of personal information to third parties is better than more. As before, though, the security against third-party eavesdropping does nothing to mitigate privacy invasions by the card issuer. Moreover, even with more sophisticated technology, security problems remain; recall the concern about whether attackers can get persistent ID from passports using the ISO 14443 chip. At best, the more sophisticated technology presents an arms race between RFID card designers and third parties seeking to hack that technology. In the words of one informed analyst, "a passport has a ten-year lifetime. It's sheer folly to believe the passport security won't be hacked in that time."[166]

V. AUTONOMY AND PUBLIC DISCLOSURE (OR: WHY SHOULD WE CARE?)

The discussion so far indicates that widespread deployment of RFID-enabled goods, credentials, or other items that move with individuals through space may present an important set of privacy threats, in particular (though not exclusively) in situations where the tag data can be read by third parties. At this point, I think it is important to devote at least a word or two to why we should view that as a problem. I will not attempt a systematic justification of privacy as a value, for that would demand a paper far longer than this one. Privacy is "a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings" that it tends to defy rigorous analysis.[167] But a key aspect

[165] *See* sources cited *supra* notes 133–36 and accompanying text.

[166] Posting of Bruce Schneier to Schneier on Security, Hackers Clone RFID Passports, http://www.schneier.com/blog/archives/2006/08/hackers_clone_r.html (Aug. 3, 2006, 15:45 PST).

[167] Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2087 (2001).

of privacy, I will posit, rests in the nature of identity and social relations in the world at large. Traditionally, we have created social relations by deciding what information about ourselves we want to disclose and to whom. Our various social relationships carry with them varying norms governing what information we disclose to others and how those others will safeguard the information we have disclosed.[168] We create concentric circles of intimacy by disclosing more (or more sensitive) things to people we are closer to and fewer to others.[169]

Our ability to calibrate our disclosures in that way is precious. At the outset, limiting disclosure about our private and social choices to people within our circles of trust allows us to make those choices without worry that they will be met with disapproval or ill-will from a larger society.[170] More fundamentally, though, my being unable to limit disclosure in that manner denies my ability to constitute and define my own social relations with others. It forces me to treat strangers as falling within one of my circles of trust or intimacy, as having some bond of relationship with me, without regard to whether that is something I would choose. My ability to disclose or withhold information has social meaning: it demonstrates that I am the owner of my own self and my own relationships. It attests that I am not someone else's data, not a specimen belonging to those who would investigate me.[171]

The profiling, surveillance, and action threats described in the previous section put these values in jeopardy. When RFID tags promiscuously broadcast a wide range of information about me to all comers, facilitating the creation of a large-scale profile possibly tied to my name, I lose my autonomy to decide for myself to whom I will

[168] *See* Nissenbaum, *supra* note 12. On the social expectations attached to others' treatment of information we have disclosed to them in particular commercial settings, *see* Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1304–11 (2000).

[169] *See* Charles Fried, *Privacy*, 77 YALE L.J. 475, 482–86 (1968); James Rachels, *Why Privacy is Important, in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 290 (Ferdinand D. Schoeman ed. 1984); *see also* Philip E. Agre, *The Market and the Net: Personal Boundaries and the Future of Market Institutions* (Oct. 6, 1998), http://polaris.gseis.ucla.edu/pagre/boundaries.html.

[170] *See* Reiman, *supra* note 153, at 35–36; Nissenbaum, *supra* note 12, at 148–49; Fried, *supra* note 169, at 483–84.

[171] The turns of phrase are from Reiman, *supra* note 153, at 39; *see* Jeffrey Reiman, *Privacy, Intimacy, and Personhood*, 6 PHIL. & PUB. AFF. 26, 39 (1976) ("Privacy is a social ritual by means of which an individual's moral title to his existence is conferred.").

disclose that information. (That remains the case even where particular individual elements of the profile are visually available to strangers in public places; the danger lies, in part, in the cheap and easy digital aggregation of all of the pieces of the puzzle that describes me.) By locating me in space and impressing my digital profile on my physical body, the technology magnifies the privacy threat. Inviting strangers to take actions regarding me, based on my constellation of tags, suppresses my ability to make my own choices in a zone of "relative insulation."[172]

VI. Policies for Near-term RFID Deployment

How—if at all—should regulators respond to the privacy threats I have described? This section of the paper will discuss policies for near-term RFID deployment. It first explains the undesirability of incorporating RFID into either driver licenses or passports. It next turns to the use of RFID in inventory control tags. The article concludes that the EPC "kill command" is unlikely to be an effective way of addressing privacy threats. Proposed data-privacy rules based on fair information practice principles, while intelligent and coherent, appear complicated and difficult to enforce; they too may be ineffective. The article suggests a simple rule that inventory-control RFID tags attached to individual items in the retail sales chain be clearly labeled and easily removable.

It is important to tread carefully before seeking to impose regulatory limits on technology. Regulation can address the negative social consequences of particular applications, but it may stifle the advance of technological knowledge in a much broader field of inquiry. Though networked sensors as a class, for example, surely present privacy risks,[173] we would hardly be well-advised at this point to dictate sweeping legal regulation of the design of sensor networks: we do not know the potential costs of such regulation, nor are we well-placed to do the line-drawing we would need.

In thinking about how best to cabin the risks presented by privacy-invasive technology, thus, we run into what one might call the Problem of Cool: how do we protect privacy without getting in the

[172] The phrase is from Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1424 (2000).

[173] *See, e.g.*, Yong Xi et al., *Preserving Source Location Privacy in Monitoring-Based Wireless Sensor Networks* (2006), *available at* http://www.cs.wayne.edu/~weisong/papers/xi06-locationprivacy.pdf.

way of the "Really Cool" functionality that the technology might at some point provide? This problem is both pervasive and intractable in privacy law; you can see it in a wide variety of contexts. Wireless location technologies have the potential for profound privacy invasion (think *Minority Report*), but can also save my life when I call 911, find me the nearest Starbuck's, and hook me up with any of my friends who happen to be in the area. Web cookies allow Doubleclick to track me from site to site, but greatly simplify the ordering process for electronic commerce, and allow the tailoring of web content in potentially Cool ways. Networked credit dossier databases may share my personally identifying information with the world, but they also enable, say, my instant mortgage approval.

In the United States, we most commonly try to address this issue through an opt-out mechanism by giving (or saying we are giving) users the opportunity to opt-out of privacy-invasive technologies if they choose. I can turn off some of my phone's wireless location features. I can reject cookies. The law encourages information proprietors to maintain privacy policies, on the theory that this will enable me to opt-out of transactions leading to my personally identifiable information being included in networked databases, available to third parties. All this is an attempt to protect privacy without intrusively regulating technology. The approach does not necessarily work especially well. Privacy policies, after all, are not particularly successful in keeping personally identifiable information out of networked databases. To the extent that a market-dominant digital rights management system, say, presents privacy threats, it is hardly clear that I can opt-out of it at reasonable cost.

Effective market power plays an important role in determining the value of opt-out approaches. The availability of alternatives is one reason why website proprietors rarely close their sites entirely to visitors refusing cookies. By contrast, to the extent that privacy-invasive digital rights management is built on Microsoft's Next-Generation Secure Computing (formerly Palladium) architecture, it will be the Wintel near-monopoly that enables that privacy invasion. Credit card companies similarly have the market power to force cardholders to abide by their privacy rules. These are the areas where U.S. privacy law tends to present harder questions or simply fails. But the opt-out approach tends to be U.S. law's first cut at the problem.

With that in mind, I want to examine some of the more specific contexts in which RFID technology may present a privacy threat. Start with government documents, because these are the easiest to analyze from the perspective of opt-out: if our government requires RFID-enabled passports (as it does), or RFID-enabled driver licenses (as it currently does not), then no opt-out is meaningfully available. It is no answer to say that somebody who wishes to avoid the privacy consequences of an RFID-enabled driver license need not get such a license, or need not carry it on his person; that is not a realistic option.

The State Department designed its RFID-enabled passports with relatively sophisticated protections against third-party access. Those protections, though, are hardly the end of the analysis. These documents incorporate personally identifying information and broadcast that information directly to reader devices. The potential they present for surveillance and tracking means that the wireless availability of the information to *authorized* government readers, without more, is worrisome from a privacy standpoint. And the possibility of attack or interception by unauthorized readers, even if it consists only of the interception of a persistent unique ID, is always present.

A DHS advisory subcommittee last year issued a report urging that the government not use RFID in connection with identification documents.[174] RFID, the report argued, does not increase the speed or efficiency of identification processes. The RFID transmission by itself, after all, provides no assurance that the person holding an RFID-equipped document is the person described in it. To get reliable identification, a government verifier must compare biometric identifiers on the document with the bearer's own characteristics—but RFID provides little help in that process. On the other side of the ledger, the report urged, the use of RFID for human identification poses privacy and security risks out of proportion to its ordinary benefits.[175]

The Department's full advisory committee on Data Privacy and Integrity, in its final report seven months later, softened its subcommittee's language somewhat, backing away from its flat statement that RFID should be disfavored for human identification. The final report, though, still made it clear that RFID-identified human identification systems did not provide clear efficiency benefits, and posed multiple privacy and security risks.[176] It urged that RFID-

[174] DEP'T OF HOMELAND SEC., THE USE OF RFID FOR HUMAN IDENTIFICATION: A DRAFT REPORT FROM THE DHS EMERGING APPLICATIONS AND TECHNOLOGY SUBCOMMITTEE V. 1.0 (2006), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_rpt_rfid_draft.pdf.

[175] *Id.*

[176] *See* DEP'T OF HOMELAND SEC., DATA PRIVACY & INTEGRITY ADVISORY COMM., REP. 2006-02: THE USE OF RFID FOR HUMAN IDENTITY VERIFICATION 4–6 (2006) [hereinafter *DHS REP. 2006-02*], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf.

enabled systems be deployed only where other technologies (such as 2-D barcodes, contact-required smartcards, or magnetic strips) could not do the job[177]; where data would be encrypted in tags, in transit, and in the database, and the chip designed so that no two communication sessions appeared alike[178]; where read ranges were no longer than necessary to accomplish the objective[179]; where there were adequate protections against secondary use of the data and the information would not be maintained longer than necessary to meet the objective for which it was collected[180]; and where, absent legitimate reason for a different implementation, individuals had opportunity to opt-out and there was a means to deactivate RFID functionality.[181]

These cautions seem entirely well-taken. The initial point—that RFID, with its attendant privacy and security risks, not be deployed absent powerful countervailing benefits—is perhaps the most immediately salient. It is hardly clear why it is desirable for passports to incorporate RFID. As the DHS committee noted, while the inclusion of digitized and encrypted information on identification documents provides important anti-forgery and anti-tampering benefits, that does not mean that the information need be transmitted *wirelessly*.[182] Other forms of transmission, such as contact chips, 2-D barcodes and optical memory stripe technology, are more secure and less vulnerable to eavesdropping and skimming.[183] The relevant International Civil Aviation Organization subcommittee (on which the United States played an active and supportive role), it appears, excluded contact chip technology for passports because there were no established standards for fabricating passports with contact chips or for reading them and because of fears that passports with contact chips would be insufficiently durable.[184] But the privacy and security

[177] *Id.* at 9.

[178] *Id.* at 11.

[179] *Id.* at 9.

[180] *Id.* at 9–11.

[181] *Id.* at 9, 11.

[182] *Id.* at 6–7.

[183] *See* Letter from the Electronic Frontier Foundation et al., *supra* note 124.

[184] *See* Electronic Passport, 70 Fed. Reg. 61,553 (Oct. 25, 2005) (to be codified at 22 C.F.R. pt. 51) (Department of State final rule on electronic passports); Posting by Bruce Schneier to

challenges RFID creates should have imposed a stronger presumption that wireless technology is the wrong way to get digital information from a passport to a government reader.

With respect to driver licenses, the key question is the same: absent any good reason why driver licenses should incorporate RFID, and given the inherent privacy risks, we need not worry about finding the most privacy-friendly RFID implementation: RFID should not be in driver licenses at all.[185] And banning RFID from driver licenses presents no meaningful risk of stifling important technological development.

What about inventory control tags? As a starting point, RFID tags on cases and pallets do not present any significant privacy threat. The privacy threat from RFID in the retail supply chain comes when tags are attached to consumer goods, on the item level; those tags leave the store attached to the item, live and serialized; and the tags are not discarded with the item's packaging.[186]

This sort of RFID implementation presents entirely different issues from, say, the RFID-enabled passport. The information stored on an inventory control tag, apart from its possible use as a persistent identifier, is often not sensitive (perhaps, a pointer to a database revealing that the tag is attached to a particular model and color of sweater). Data security, on the other hand, is essentially nonexistent. Some of the privacy threat here comes from the possibility that individuals may find themselves, at one time or another, carrying a

Schneier on Security, Hackers Clone RFID Passports (quoting Randy Vanderhoof, Executive Director, Smart Card Alliance), http://www.schneier.com/blog/archives/2006/08/hackers_clone_r.html#c99421 (Aug. 3, 2006, 15:45 PST).

[185] *See* ACLU Testimony on Computer Chips in Virginia Drivers Licenses: Testimony Before the Virginia Legislature on House Joint Resolution 162, Considering the Creation of Smart Driver's Licenses (Oct. 6, 2004), *available at* http://www.aclu.org/Privacy/Privacy.cfm?ID=16658&c=39 (testimony of Chris Calabrese, Program Counsel for ACLU's Technology and Liberty Program).

[186] *See* PAPPU, *supra* note 151. It is true that if manufacturers deploy item-level tags that do not leave the store, consumers might still be subject to some sort of surveillance as they interact with the tags inside the store. *See id*; CASPIAN ET AL., *supra* note 11, at 8–9. But I see that threat as relatively minor. The technology in this context would not identify customers, facilitate profiling, or enable any meaningful action threat, unless the store were able to identify customers in some entirely separate manner, such as by taking pictures using in-store cameras. Stores have in fact used RFID in conjunction with cameras in tests. *See* Alorie Gilbert, *Cutting-Edge 'Smart Shelf' Test Ends*, CNET NEWS.COM, Aug. 22, 2003, http://news.com.com/2100-1008_3-5067253.html; Howard Wolinsky, *P&G, Wal-Mart Store Did Secret Test of RFID*, CHI. SUN-TIMES, Nov. 9, 2003, at 36 (but in those cases cameras posed the main privacy threat, one not appreciably augmented by the use of RFID).

variety of tags and thus at the center of a buzzing swarm of small information transfers that can be aggregated into a much larger whole. The remaining privacy threat comes from the possibility that, once a unique ID on a tag is linked to an individual's personal identifying information, the tag for surveillance purposes is equivalent to a device transmitting the identifying information directly.

At the outset of the privacy debate over RFID in this context, EPCGlobal (the trade body that stepped into the shoes of the Auto-ID Center as the standards body for RFID in the retail sales chain) came forward with an opt-out-based approach to privacy protection: the "kill command." Under EPCGlobal's specifications, inexpensive passive RFID tags are designed to respond to a password-protected command directing the tag's integrated circuit to disable itself. Retailers thus can choose to allow consumers to have RFID tags on their purchases disabled before they leave the store.[187]

There is appeal to the "kill command." The option of killing retail tags at the point of sale recognizes the different tradeoffs the technology presents at different points in the retail-goods' life cycle. While goods are moving through the retail sales chain, RFID tagging can offer important inventory-control benefits, with essentially no cost in terms of consumer privacy. Once the good is sold to the consumer, by contrast, there is no further need for inventory control. Moreover, the approach EPCGlobal contemplates—that at the point of sale the consumer would have the option to ask that a tag be disabled—allows the consumer to maintain the functioning tag if it sees benefit in that course.

EPCGlobal's approach, however, has the flaw all too often present in opt-out solutions: it seems unlikely to do a very good job of actually keeping live tags off the streets. It is by no means clear that manufacturers (who will be the firms actually purchasing and affixing tags in the retail sales chain) are interested in enabling the kill capability.[188] More importantly, retailers are unlikely to want to incur

[187] The kill functionality is also included in EPCGlobal's second-generation protocol specification. *See* Rajendra Chaudhary, *ISO Says Yes to EPC Gen2*, CXOTODAY.COM, July 25, 2006, http://www.cxotoday.com/cxo/jsp/article.jsp?article_id=74813&cat_id=912.

[188] It is not clear to what extent major manufacturers of retail goods were ever interested in this kill functionality. According to one source, those users were split. Some were willing to enable killable tags as an option for consumers; others, such as Nestle, were not. Those others were unwilling to give up the potential functionality of tags that continue to operate past the point of sale (facilitating returns and the like), and believed that privacy advocates represented a minority who in the end would be unable to stop the technology's rollout. *This Month's Summary*, RFID ANALYST 4–5 (April 2004) (RFID ANALYST was formerly SMART LABELS ANALYST).

the additional expense associated with allowing customers to kill tags. Small retailers in particular, who may find it cheaper to continue counting inventory by hand than to invest in smart shelves or a reader network, will be reluctant to buy expensive equipment to disable the RFID tags they will be receiving, uninvited, on their consumer packaged goods.[189]

Even if the law should require that consumers be offered a kill option, consumers may not exercise that option if disabling the tag requires more time at checkout or other inconvenience for the consumer. That is all the more true if retailers or manufacturers offer consumers any sort of incentive to forgo disabling their tags, such as a more convenient return policy. Consumers tend to underestimate the incremental impact on their privacy of allowing just one more set of small disclosures, in part because they are not fully aware of the degree to which any given disclosure can become part of an aggregate, data-mined profile.[190] Many will take the path of least resistance, not bothering to opt out from the privacy-invasive default. Once a large number of consumer goods with live EPC tags make it onto the streets, we have to confront the fact that these tags, at least as currently imagined, incorporate no useful privacy protections. As with government documents, thus, opt-out does not provide a very satisfactory answer.

Are there other solutions? A number of government and private organizations have suggested best practices for inventory control RFID. These tend to be based, in greater or lesser degree, on the fair information practice principles[191] that, though only sporadically reflected in U.S. law, play an important role in U.S., as well as

[189] *See* STAPLETON-GRAY, *supra* note 68.

[190] *See* Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1072–74 (1999).

[191] One good summary of Fair Information Practice principles can be found in the Federal Trade Commission's 1998 *Privacy Online: A Report to Congress*: (1) consumers should get notice of an entity's privacy policies before that entity collects any personal information from them; (2) consumers should be able to choose whether to convey the information, and how it can be used or transferred; (3) consumers should be able to see the information collected about them, and to contest its accuracy or completeness; (4) the collector must take reasonable care that the information it maintains is accurate and secure; (5) there must be some mechanism, other than the data collector's good intentions, to bring about compliance. U.S. FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS III.A (1998), http://www.ftc.gov/reports/privacy3/fairinfo.htm#Fair%20Information%20Practice%20Principles; *see FTC RFID Workshop*, *supra* note 20, at 275–76 (testimony of Cedric Laurant, Policy Counsel, Electronic Privacy Information Center).

European information privacy thinking.[192] Fair information practice principles are not, in fact, obviously well-suited to data collection systems like simple RFID. These principles work best in systems with clearly identified data collectors, who have the information because the consumer has voluntarily given it to them in order to facilitate some transaction the consumer wants, and who are subject to meaningful restraints on information reuse and sharing. But the architecture of unsophisticated RFID systems allows anyone, including persons entirely unrelated to the tag's manufacturer or its intended users, to be a data collector. Reading is undetectable, and nothing will cause the consumer to know that a reader is collecting data about him. Data collection may be the basis of privacy threats even though the information is never linked to the subject's name.[193] Fair information practice principles work less well in systems in which devices reveal information indiscriminately, so that there is no way to identify a class of information collectors who can be made subject to the rules.

They are not completely inapposite, though. As I noted earlier, the worst RFID privacy threats come when tag data can be linked to an individual's name or other personal identifying information.[194] Fair information practices can be used to address that linkage. A regulator, or a set of industry best practices, might discourage entities operating RFID technology from linking tag IDs to personally identifying information. It might allow such linkage only in limited circumstances, or request the data collector to disclose the fact and purpose of the linkage to the individual involved and to obtain her written consent. Further, it might forbid the data collector to disclose that linkage to any unaffiliated third party. All of these suggestions can be found in the Electronic Privacy Information Center's ("EPIC") proposed guidelines for commercial use of RFID.[195] The EPIC

[192] The first proposal for RFID privacy guidelines based on fair information practice principles, to my knowledge, was SIMSON GARFINKEL, ADOPTING FAIR INFORMATION PRACTICES TO LOW COST RFID SYSTEMS (2002), *available at* http://www.simson.net/clips/academic/ 2002.Ubicomp_RFID.pdf.

[193] *See* PAMELA SAMUELSON, SENSOR NETWORKS & PRIVACY 8 (Mar. 13, 2004), *available at* http://www.sims.berkeley.edu/~pam/papers/Stanford%20cybpriv.ppt (slides presented at Stanford Law School Symposium: Securing Privacy in the Internet Age).

[194] *See* sources cited *supra* notes 157–59 and the accompanying text.

[195] *See* CÉDRIC LAURANT & KENNETH FARRALL, COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER TO THE FEDERAL TRADE COMMISSION 17–18 (2004), *available at* http://www.epic.org/privacy/rfid/ftc-comts-070904.pdf; *see also FTC RFID Workshop*, *supra* note 20, at 205 (testimony of John Parkinson, Vice President and Chief Technologist,

guidelines also seek to impose restrictions on tag data collection to minimize the respects in which RFID makes fair information practice principles problematic, by prohibiting the use of tag readers except where individuals have been warned that they are present, and by requiring that readers emit a tone or light, or some other easily recognizable indicator, when they draw information from RFID tags.[196]

A working group assembled by the Center for Democracy and Technology, including a variety of industry actors such as Procter & Gamble, Intel, Verisign, and Microsoft, developed a different set of best practices, stating that consumers should be provided with notice when information is collected through an RFID system and is linked, or is intended by a commercial entity to become linked, to an individual's personal information. The notice should specify why the linked information is being collected and how it will be used; consumers should be given the choice to refuse consent for uses other than enabling the functioning or delivery of a purchased device or contracted service, or facilitating the completion of the business transaction. On the other hand, businesses need not give notice if, in their "judicious discretion," they determine that the ease and likelihood of linkage is sufficiently attenuated as to lower the privacy risk.[197]

The European Commission ("EC") has launched an ongoing consultation on RFID policy, with a Communication from the Commission expected in the spring of 2007.[198] An earlier EC Working Party published a document in 2005 and took the position that existing European data protection law covers the collection of RFID data whenever that information either contains personal information or is reasonably likely to be linked to it.[199] In those

Capgemini) ("Control of the object name servers and how you get to the intelligence that tells you what [a tag ID] means should be the primary place to start applying policy.").

[196] *See* LAURANT & FARRALL, *supra* note 195, at 17.

[197] CTR. FOR DEMOCRACY & TECH., CDT WORKING GROUP ON RFID: PRIVACY BEST PRACTICES FOR DEPLOYMENT OF RFID TECHNOLOGY (May 1, 2006) (interim draft), *available at* http://www.cdt.org/privacy/20060501rfid-best-practices.php.

[198] *See* RFID Consultation Website, http://www.rfidconsultation.eu/ (last visited Jan. 17, 2008).

[199] ARTICLE 29 DATA PROTECTION WORKING PARTY, WORKING DOCUMENT ON DATA PROTECTION ISSUES RELATED TO RFID TECHNOLOGY 8 (2005), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp104_en.pdf. It was anticipated by a ruling by Portugal's National Data Protection Commission that RFID data collection is subject to that nation's data privacy laws. *See Portuguese Commission Rules*

situations, the report continues, data controllers are obligated to comply with ordinary European data protection principles: data must be used only for the purposes for which it was collected, not excessive for that purpose, and kept no longer than necessary. In most circumstances, it can be collected only on the basis of specific, unambiguous informed consent. Data subjects must have notice of the identity of the data collector and the purposes of the collection. They must be told how to remove or disable RFID tags. And they must have access to any information being kept about them.[200]

The EC working document notes that RFID technology may make some of these limitations difficult to enforce. It may be difficult to monitor the purposes for which linked data is used, or even to know which parties are maintaining data about a subject.[201] The EC Working Party thus concluded, as a general matter, that data subjects must have notice of the presence of RFID tags and readers, as well as the consequences of that presence in terms of information gathering.[202]

I have to confess dissatisfaction, though, with these suggestions and best practices guides. My dissatisfaction stems from two sources. First, the various proposed rules tend to be complicated and difficult to enforce. They will not, individually or together, necessarily be effective at addressing the dangers presented by citizens' and consumers' walking around with live, unsophisticated, serialized tags. Second, I suspect that the "Cool" post-sale uses of item-level inventory-control RFID tags will be few; manufacturers' reluctance to

RFID Use Subject to Country's Data Protection Law, 13 Telecomms. Monitor (BNA) (Jan. 22, 2004).

[200] ARTICLE 29 DATA PROTECTION WORKING PARTY, *supra* note 199, at 9–11. The RFID privacy guidelines published by Ontario's Information and Privacy Commissioner similarly focus on the link between tag data and personally identifying information. Following the general outlines of fair information practices in other contexts, those guidelines provide that organizations must seek individual consent prior to collecting, using, or disclosing personal information linked to an RFID tag. They may link RFID data to personally identifiable information covertly, indiscriminately, or through deception. They should collect no more than the minimum information necessary to effectuate the purposes they have disclosed to the consumer, and must destroy that information once it is no longer necessary to effectuate those purposes. They should minimize the identifiability of any personal data linked to a tag, minimize tags' vulnerability to reading by third parties, and minimize the linkability of collected data to any personally identifiable information. Finally, they may not use, disclose, or link to a consumer's personal information for any new purposes without the consumer's consent.

[201] *See id.* at 13.

[202] *See id.* at 10.

expose tag data to the world via the ONS will make it harder for third parties to offer useful post-sale functionality. By contrast, if such tags are widely deployed, the possible privacy-invasive uses of such tags once goods are sold will be many–that is the direction that economic incentives push in.

This suggests that we would do well to adopt a simple rule requiring that inventory-control RFID tags attached to individual items in the retail sales chain be clearly labeled and easily removable.[203] That should not pose an insuperable barrier for industry; EPCGlobal's best practice guidelines for RFID tags on consumer products "anticipate[] that for most products," tags will be "part of disposable packaging or . . . otherwise discardable."[204] Alternatively, retailers could rely on technology like the IBM Clipped Tag.[205] The Clipped Tag is perforated. After purchasing a tagged item, a consumer can tear the tag along the perforations to remove part of its antenna, reducing its read range from tens of feet to a few inches. This provides an easy and visible way of disabling most remote read capability, while still preserving the serialized ID for uses such as returns (so that, say, a consumer could return an item without proof-of-purchase by virtue of the store's having associated the sale price and buyer's name with the tag ID in its database at point of sale).[206]

It is true that if manufacturers eschewed technology like the Clipped Tag and simply made tags visible and easily removable, then consumers would have to choose between privacy protection and post-sale tag functionality. If a consumer discarded a tag, she would not get the benefit of a retailer's use of RFID to facilitate returns. Recycling centers would not be able to rely on EPCs to categorize recycled items. Consumer items such as stoves and washing machines would not be able to read tag information to get cooking or washing instructions.[207]

[203] *See* LAURANT & FARRALL, *supra* note 195, at 14; *see also FTC RFID Workshop*, *supra* note 20, at 190 (testimony of Beth Givens, Director, Privacy Rights Clearinghouse). This rule would not apply if a tag were sophisticated enough to implement privacy protection, or if it carried only a generic (not globally unique) identifier.

[204] EPCGlobal, Guidelines on EPC for Consumer Products, http://www.epcglobalinc.org/public/ppsc_guide (last visited Jan. 17, 2008).

[205] *See* Ann Bednarz, *IBM Demos RFID Tag with Privacy-Protecting Features*, NETWORK WORLD, May 1, 2006, http://www.networkworld.com/news/2006/050106-ibm-rfid-privacy.html?fsrc=rss-rfid.

[206] *See id.*

[207] These uses are from ARI JUELS ET AL., THE BLOCKER TAG: SELECTIVE BLOCKING OF RFID TAGS FOR CONSUMER PRIVACY 3 (2003), *available at* www.rsasecurity.com/rsalabs/staff/bios/

Yet that result is not too distressing. Consumers would be able to retain tags when they chose to.[208] Manufacturers would remain free, if they chose, to incorporate information more permanently into consumer goods via a non-wireless bar code, or a generic tag not carrying a globally unique identifier.

To be sure, the industry is not going to adopt my proposal, at least not across the board. The Center for Democracy and Technology best practices discussed earlier were developed with industry participation, and they represent as much as the industry is willing to agree to on its own. Those best practices are rather less restrictive than my suggestion: they provide only that businesses, most of the time, ought to allow consumers to decline consent for the business's linkage of information it collects via RFID tags to the consumer's personally identifiable information. But notwithstanding that my proposal will not be adopted, it seems the simplest solution to the problem.

VII. RFID AND THE MORE DISTANT FUTURE

So far I have discussed two relatively concrete sets of RFID implementations, either already deployed or plausible in the near future, that we know a fair amount about. But what about broader concerns? It is possible to imagine a world in which RFID technology was so bound into the basic fabric of society that it would be impossible to opt-out; Sterling's vision of a world shot through with RFIDs and networked sensors, all leaving information trails and microhistories of the objects to which they are attached, comes to mind.[209]

Even if one is not willing to be that speculative, government documents and inventory control tags hardly exhaust the universe of

ajuels/publications/blocker/blocker.pdf. Juels and his co-authors urge that the ONS architecture should facilitate the use of "blocker tags," consumer-controlled devices that could be programmed to prevent the detection of particular categories of tags in a consumer's possession. All other things being equal, it would plainly be better for consumers to have access to blocker tags than not. To the extent that the tags' availability would tend to relieve any pressure to find other RFID privacy solutions, though, the emphatically opt-in nature of an approach requiring that consumers maintain their own privacy protection devices is disturbing. If consumer inertia would be a problem in connection with a right to disable tags at point of sale, it would surely be a problem here.

[208] For what it is worth, I imagine that retailers would likely take returns from consumers who remove but retain their tags, just as they take returns from consumers who present analogous documentation today.

[209] *See* STERLING, *supra* note 1, at 12–13, 45–47, 97–105.

RFID uses. The sort of RFID privacy threats I have discussed come only from items people carry, but those items also include, say, company credentials, student IDs, keys, credit and debit cards, parking cards, and transit cards. All of these, if RFID-enabled, may present privacy threats. For that matter, I have not discussed library books, tagging of postal mail and luggage, or toll-booth payment cards. All of these uses are either deployed or plausible. None have achieved a commanding position in the marketplace, but that may just be a matter of time. And with regard to all of these uses, the threats I identified in Section IV are potentially important and salient.

I believe, indeed, that in the longer term we are sliding into a world in which objects' wireless self-identification will become much more routine and networked devices will be in a position routinely to collect and process the resulting information, untouched by human hands. That is not unequivocally a bad thing: increased use of wireless technology will happen because that technology offers capabilities and efficiencies unavailable without it. But the privacy consequences, for all the reasons set out earlier in this article, may be profound.

The implementations I have described here are varied. We do not know remotely enough about them to craft a one-size-fits-all response that would make sense. It is here that the Problem of Cool is at its most acute; regulation of such a large and poorly-defined class of RFID uses poses an obvious danger of inadvertent suppression of desirable technology. Should we do nothing, then? There are costs associated with inaction, as well. As systems are deployed, they create facts on the ground. As the deployment of privacy-invasive technology makes us more accustomed to privacy invasions, those privacy invasions come to seem more natural and reasonable. The longer policymakers wait after such systems are deployed, the more industry players have a vested stake in the technology already out there and can point to regulation's disruption of reasonable investment-backed expectations.

It is widely accepted in the privacy community, moreover, that the best way to integrate privacy-invasive technologies into society is to design privacy in from the start–to design the technological implications with privacy in mind, rather than designing the technology first and thinking about privacy only afterwards.[210] So the time to be thinking about these issues is now.

[210] *See, e.g.*, *DHS Rep. 2006-02*, *supra* note 176 ("[p]rivacy and security must be built into the full lifecycle of the RFID application from the outset–from the design stage, to deployment and use, to end of life.").

The privacy community, to date, has directed extensive advocacy efforts at particular concrete RFID threats–most importantly, the inclusion of RFID in government credentials and the penetration of RFID-enabled inventory control tags into public space. They were right to do so: those threats were the most immediately problematic and had potentially huge scale. Scale is especially important in this context, since, as I noted in Section IV of this article, the most important RFID privacy dangers only come with scale. One of the issues in Section IV was whether individuals equipped with various RFID tags on their persons would really have to worry about tag information being collected by a pervasive reader network; I answered that as RFID implementations became widespread, leading a variety of commercial and governmental users to deploy a large number of smaller, discrete reader networks, economic and political incentives for sharing of information among those networks would give us the functional equivalent of a single very large network.[211] But the key to that scenario is pervasive deployment of RFID technology; if it turns out that we see only scattered deployment of occasional RFID implementations, then we will get only scattered installation of occasional RFID readers. So the largest-scale uses are especially important.

We will see how events continue to unfold with regard to the inclusion of RFID in government credentials and the penetration of RFID-enabled inventory control tags into public space. In the government sector, the key issue is the expansion of tagging beyond the passport. The most immediate battleground is DHS's ongoing process regarding the design of its PASS card.[212] In the retail sector, we need to keep our eyes out for RFID tags on individual high-value retail items, where the tags are not designed to be conspicuous and easily removable.

Those two areas, though, are not the only ones we need to think about. On the contrary, our most important challenge right now is to figure out where the rest of the universe of actual and potential RFID implementations is heading. What sort of tags will be walking around in the world of five and ten years from now? What information will they contain and what security will they carry? If we can figure those issues out, then the analysis set out earlier in this paper will help us

[211] *See* CASPIAN ET AL., *supra* note 11, at 6 and accompanying text.

[212] *See* sources cited *supra* notes 120–22 and accompanying text.

determine how to mitigate associated privacy threats. But the time to work out those answers is now.

VIII. CONCLUSION

RFID deployment to date presents something of a paradox. On the one hand, RFID is in many ways a tremendously powerful enabling technology with a wide range of potential applications. On the other hand, in the United States at least, the highest-volume applications have not yet generated a business case suggesting the sort of return on investment that would make the project worthwhile. That is most notably true in the context of inventory control; the complexity and cost of deployment, as well as the entrenched nature of existing bar-code-based tracking systems, have left many firms unenthusiastic about adopting the technology. In the end, I believe, we will find ourselves moving in the direction of a world with pervasive RFID: a world in which objects' wireless self-identification will become much more nearly routine and networked devices will be in a position routinely to collect and process the resulting information.

RFID-equipped goods and documents may reveal information about themselves, and hence about the people carrying them, wirelessly to people whom the subjects might not have chosen to inform. That information leakage follows individuals through space and reveals how they move through space. Not only does the profile that RFID technology helps construct contain information about where the subject is and has been, but RFID signifiers travel with the subject in the physical world, conveying information to devices that otherwise would not recognize her and that can take actions based on that information. RFID implementations, thus, can present three related privacy threats: geographic surveillance, profiling, and action.

RFID privacy consequences will differ in different implementations. It would be a mistake to conclude that an RFID implementation will pose no meaningful privacy threat because a tag does not directly store personally identifiable information, instead containing only a pointer to information contained in a separate database. Aside from any privacy threats presented by the database proprietor, privacy threats from third parties will depend on the extent to which those third parties can buy, barter, or otherwise gain database access. Moreover, even without database access, pointers present the danger of the data on the tag serving as a persistent unique identifier of the person carrying it.

Where a tag (such as an item-level retail inventory control tag) neither points to nor carries personal identifying information, the extent of the privacy threat will depend in part on the degree to which data collectors will be able to link tag numbers with personally identifying information. Yet, as profiling accelerates in the modern world, aided by the automatic, networked collection of information, information compiled by one data collector will increasingly be available to others as well; linking persistent identifiers to personally identifying information may turn out to be easy. Nor are sophisticated access controls and other cryptographic protections a complete answer to RFID privacy threats. The cost of those protections will make them impractical for many applications, though, and even with more sophisticated technology, security problems will remain.

RFID on inventory control tags presents important societal benefits. It is easy to exaggerate, though, the value of preserving the capability to keep such tags live after the point of sale. Society would be well served by a rule requiring that inventory-control RFID tags attached to individual items in the retail sales chain be clearly labeled and easily removable.

Turning to the government document context: by virtue of the serious privacy threats they pose, it is almost always undesirable for government identity credentials to incorporate RFID. While the inclusion of digitized and encrypted information on identification documents does provide important anti-forgery and anti-tampering benefits, that information need not be transmitted wirelessly.

What about company credentials, student IDs, keys, credit and debit cards, parking cards, and transit cards? Library books, tagging of postal mail and luggage, and toll-booth payment cards? These have been less examined, but all of them, if RFID-enabled, may present privacy threats. We need to figure out what to expect from the future of RFID implementations: what sort of tags will be walking around in the world of five and ten years from now; what information they will they contain, and what security they will they carry. Those answers are crucial if we are to be able to address the privacy threats that—without careful and mindful design—RFID will pose.