

# RFID and Privacy

Jonathan Weinberg\*

RFID is hot. The Transportation Security Agency is talking about RFID-tagged airline boarding passes that, its officials hope, would allow security personnel to track all passengers' whereabouts, in real time, throughout every airport.<sup>1</sup> The Food and Drug Administration has called for RFID tags on every package of prescription drugs.<sup>2</sup> Wal-Mart and other major retailers are demanding that their top suppliers have pilot RFID implementations in place before this book sees print.<sup>3</sup> The State Department is implementing plans to incorporate RFID in U.S. passports.<sup>4</sup> One company has announced a "secure, subdermal RFID payment technology for cash and credit transactions" — consumers will have the chip implanted in the triceps area, and make payments by passing a scanner over their arms.<sup>5</sup> After all, the company urges, this way the payment device will be impossible to lose.<sup>6</sup>

Current discussion and implementation of RFID reflects a lot of hype, and more than a little herd mentality;<sup>7</sup> RFID's momentum in the marketplace, though, is real. In this paper, I will briefly describe RFID technology; speak to its likely trajectory and diffusion; analyze the privacy threats it poses; and discuss some possible answers.

---

\* Professor of Law, Wayne State University. I am indebted to 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, held at the University of Ottawa on October 4, 2003; and most of all to 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 for her insightful comments.

<sup>1</sup> Bob Brewin, TSA eyes RFID boarding passes to track airline passengers, *Computerworld* (Apr. 1, 2004), <<http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,91830,00.html>>. (No, this doesn't appear to have been an April Fools' joke.)

<sup>2</sup> See U.S. Food & Drug Administration, COMBATING COUNTERFEIT DRUGS § D.1.e (Feb. 2004), <[http://www.fda.gov/oc/initiatives/counterfeit/report02\\_04.html#radiofrequency](http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html#radiofrequency)>.

<sup>3</sup> Wal-Mart has directed its top suppliers that, as of January 2005, each of the pallets and cases those suppliers ship to certain Wal-Mart distribution centers should have readable RFID tags. See Carol Sliwa and Bob Brewin, RFID Tests Wal-Mart Suppliers, *Computerworld* (Apr. 5, 2004), <<http://www.computerworld.com/softwaretopics/erp/story/0,10801,91913,00.html>>.

<sup>4</sup> See Edward Hasbrouck, Time to get a new USA passport, *The Practical Nomad* (Oct. 14, 2004), <<http://hasbrouck.org/blog/archives/000433.html>>.

<sup>5</sup> See Press Release, Applied Digital Solutions' CEO Announces "Veripay™" Secure, Subdermal Solution for Payment and Credit Transactions at ID World 2003 in Paris (November 21, 2003), <<http://www.adsx.com/news/2003/112103.html>>.

<sup>6</sup> "[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." *Id.* (internal quotation marks omitted).

<sup>7</sup> See David Margulius, The Rush to RFID, *Infoworld* (Apr. 9, 2004), <[http://www.infoworld.com/pdf/special\\_report/2004/15SRrfid.pdf](http://www.infoworld.com/pdf/special_report/2004/15SRrfid.pdf)> (quoting Jon Brendsel, director of electronic product code network services, VeriSign).

## I.

The term RFID (or **R**adio **F**requency **I**dentification) 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.

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, and the reader design, as well as of 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,<sup>8</sup> 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 FCC regulation), its antenna gain (ditto), 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 20 meters between tag and reader.<sup>9</sup> Distances actually achievable in the field are typically much shorter; one industry expert describes ten meters as the “best case scenario[] today,” and suggests that a typical operating environment features a read range of three to five meters.<sup>10</sup>

Various firms and governments are currently planning, and putting into place, a wide range of RFID implementations. The Auto-ID Center at the Massachusetts Institute of Technology recently 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 is continuing its standards efforts under the EPCglobal organizational structure.<sup>11</sup> In

---

<sup>8</sup> An “active” RFID tag, by contrast, is powered by an internal battery.

<sup>9</sup> See Matt Reynolds, The physics of RFID, <<http://www.rfidprivacy.org/papers/physicsofrfid.pdf>> (Nov. 15, 2003).

<sup>10</sup> Radio Frequency Identification Applications and Implications for Consumers. Hearing before the Federal Trade Commission (June 21, 2004) [hereafter FTC RFID Workshop] 23-34 (testimony of Daniel Engels, Executive and Research Director, Auto-ID Labs); see also *id.* at 35 (testimony of Manuel Albers, Phillips Semiconductor) (describing six meter read range on inexpensive cards); *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”).

<sup>11</sup> See What’s in a Name?, AIM Global, <<http://www.aimglobal.org/technologies/rfid/resources/articles/oct03/name.htm>>. EPCglobal is a joint venture of EAN International and the Uniform Code Council, which administer the bar code system today. *Id.*; see also FTC RFID Workshop, *supra* note 10, at 269-70 (testimony of Elizabeth Board, EPC Public Policy Action Committee).

the Auto-ID Center / EPCglobal architecture, each tag includes a globally unique Electronic Product Code (EPC) that in turn points to an entry in a worldwide distributed database called the Object Name Service.<sup>12</sup>

The Auto-ID Center / EPCglobal architecture is directed at RFID's most commercially important implementation: inventory management. Each pallet or case of consumer goods -- indeed, each individual item -- can have affixed an inexpensive passive RFID tag holding an EPC. 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.

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,<sup>13</sup> 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, or automobile transmission, or can of beans.<sup>14</sup>

A number of large retailers are pushing hard to implement RFID tagging in their supply chains on the case and pallet level. They urge that the ability to track cases and pallets wirelessly and automatically will give them a better picture of where manufactured items are in the supply chain and how fast it takes them to get there, enabling them to be more efficient in moving goods through the distribution process and making sure they're where they need to be.<sup>15</sup> Retail industry analysts urge that 6-10% of spending on the supply chain is lost due to lack of visibility or poor visibility in the supply chain; they believe that RFID will address that.<sup>16</sup>

---

<sup>12</sup> 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.

<sup>13</sup> On the other hand, some barriers, particularly metal and fluid-rich substances such as the human body, may disrupt the radio signal. See *infra* text at notes **Error! Bookmark not defined.-Error! Bookmark not defined.**

<sup>14</sup> These differences recently led the Senate Judiciary Committee's ranking member to call RFIDs "barcodes on steroids." Remarks of Senator Patrick Leahy, 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>>.

<sup>15</sup> FTC RFID Workshop, *supra* note 10, at 13-14 (testimony of Sue Hutchinson, product manager, EPCglobal).

<sup>16</sup> *Id.* at 52-53 (testimony of Britt Wood, Senior Vice President, Retail Industry Leaders Ass'n); <<http://www.ftc.gov/bcp/workshops/rfid/wood.pdf>>, at 4.

Wal-Mart, thus, has 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 plans to expand the program to a dozen distribution centers and up to 600 stores by January 2006.<sup>17</sup> The move is evocative of Wal-Mart's leading role in causing suppliers to adopt old-fashioned bar codes in the mid-1980s<sup>18</sup>; by 2007, suppliers will likely be moving in lock-step with Wal-Mart in tagging pallets and cases of retail goods.<sup>19</sup> In Great Britain, supermarket chain TESCO has announced ambitious plans for case- and pallet-level RFID in its supply chain.<sup>20</sup> European retailing giant Metro plans an RFID rollout that by December 2005 will include 100 suppliers, 269 stores, and eight distribution centers.<sup>21</sup> Back in the United States, Target and Albertson's have announced their own, comparable, tagging plans,<sup>22</sup> and other large retailers are set to follow.<sup>23</sup> The U.S. Department of Defense is seeking to require all suppliers by January 2005 to put passive RFID tags on "the lowest possible part, case or pallet packaging."<sup>24</sup> Wal-Mart's push, and the continuing buzz over RFID in the marketplace, is causing 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 fear they'll be left behind if they don't.

The buzz over RFID isn't limited to the case and pallet level. A variety of companies have engaged in *item-level* testing of tags on a broad range of consumer goods. That is, their trials involve the placement of tags on individual consumer items. Benetton made plans early to

---

<sup>17</sup> FTC RFID Workshop, *supra* note 10, at 120 (testimony of Simon Langford, Manager of RFID Strategy, Wal-Mart). But see *id.* at 223-24 (testimony of Chris Boone, program manager, IDC) (Wal-Mart suppliers will probably only be in partial compliance by January 2005).

<sup>18</sup> See Scott Granneman, RFID Chips Are Here, *The Register* (June 27, 2003), <[http://www.theregister.co.uk/2003/06/27/rfid\\_chips\\_are\\_here/](http://www.theregister.co.uk/2003/06/27/rfid_chips_are_here/)>.

<sup>19</sup> FTC RFID Workshop, *supra* note 10, at 225 (testimony of Chris Boone, program manager, IDC).

<sup>20</sup> Jo Best, Tesco takes RFID into all Extra superstores, *Silicon.com* (Sept. 30, 2004), <<http://networks.silicon.com/lans/0,39024663,39124558,00.htm>>.

<sup>21</sup> Jo Best, Retailer to follow RFID test with full rollout, *CNET* (September 3, 2004), <<http://asia.cnet.com/news/systems/0,39037054,39192342,00.htm>>.

<sup>22</sup> FTC RFID Workshop, *supra* note 10, at 224 (testimony of Chris Boone, program manager, IDC); Josh McHugh, Attention, Shoppers: You Can Now Speed Straight Through Checkout Lines!, *Wired* 12:07 (July 2004), <<http://www.wired.com/wired/archive/12.07/shoppers.html>>.

<sup>23</sup> See Jacqueline Emigh, More Retailers Mull RFID Mandates, *eWeek* (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").

<sup>24</sup> 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!, *Federal Computer Week* (Nov. 3, 2003), <<http://www.fcw.com/fcw/articles/2003/1103/pol-dod-11-03-03.asp>>; see also Matthew French, Military releases RFID policy, *Federal Computer Week*, (Oct. 24, 2003), <<http://www.fcw.com/fcw/articles/2003/1020/web-rfid-10-24-03.asp>>.

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. Other companies, however, seem undeterred. Marks & Spencer has conducted two trials of item-level RFID tags in menswear, and appears committed to item-level RFID as a stock control system. It emphasizes that its tags are large, visible, and easily removed by the consumer.<sup>25</sup> At least one major U.S. clothing manufacturer, it appears, may be planning to incorporate item-level RFID tags into its clothing in 2005; currently available evidence suggests that those tags may be quite difficult to notice, and may well be retained in the garment by the unsophisticated consumer.<sup>26</sup>

Michelin has begun fleet testing for RFID for passenger & light truck tires. Each tire's unique identification number will be associated in an external database with the Vehicle Identification Number (VIN) of the car on which it's mounted, and with information describing when and where the tire was made, its maximum inflation pressure, its size, and so on.<sup>27</sup>

Gillette (which announced in early 2003 that it would purchase 500 million RFID tags)<sup>28</sup> has 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, the data proprietor would always know how many packages are on the shelves, without having to count them.

Casinos are putting RFID tags in chips to block counterfeiting, identify stolen chips, and track gamblers' play. An Italian manufacturer has introduced a washing machine equipped to read RFID washing instruction tags in clothing.<sup>29</sup> 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.

---

<sup>25</sup> FTC RFID Workshop, *supra* note 10, at 265-68 (testimony of James Stafford, Head of RFID, Marks & Spencer). Marks & Spencer has also deployed three and a half million RFID tags on its returnable food trays, which cycle between the store and its food suppliers. *Id.* at 263-64.

<sup>26</sup> See CASPIAN, Mystery Clothing Company Plans Item-level RFID Rollout (Sept. 23, 2004), <<http://www.spsychips.com/press-releases/checkpoint.html>>; CASPIAN, Which company has secret, item-level RFID tagging plans? (Sept. 23, 2004), <<http://www.spsychips.com/press-releases/checkpoint-photos.html>>.

<sup>27</sup> See Michelin Introduces Radio Frequency Tire Identification Technology, Motor Trend (Jan. 16, 2003), <[http://www.motortrend.com/features/news/112\\_news011603\\_tire/](http://www.motortrend.com/features/news/112_news011603_tire/)>.

<sup>28</sup> See David Ewalt, Gillette Orders 500 Million RFID Tags, Information Week (Jan. 6, 2003), <<http://www.informationweek.com/story/IWK20030106S0007>>.

<sup>29</sup> See Merloni Unveils RFID Appliances, RFID Journal (April 4, 2003), <<http://www.rfidjournal.com/article/articleview/369/1/1/>>. A variety of automobile manufacturers, indeed, currently incorporate RFID into the ignition key, so that the key can identify itself to the anti-theft system. See FTC RFID Workshop, *supra* note 10, 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).

It's possible to imagine a whole lot of uses, indeed, for a technology in which objects can be uniquely identified without direct contact. This is the ideal technology if you want the milk in your refrigerator to notify you (or your supermarket) if you've failed to drink it by its pull date.<sup>30</sup> Indeed, you could tie a slightly more elaborate tag to a nanosensor that checks for spoilage directly.<sup>31</sup>

One can implant RFID tags into people, subcutaneously. The FDA has approved the implantation into human subjects of RFID tags referencing the subjects' medical records.<sup>32</sup> A Spanish nightclub has gone ahead and injected RFID tags into some of its customers, who thereby got free access to the club's VIP area.<sup>33</sup> 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."<sup>34</sup> Subcutaneous chipping seems to have caught on in Mexico: The country's attorney general announced this summer 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 "anywhere inside Mexico" in the event of assault or kidnapping.<sup>35</sup> (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.) 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.<sup>36</sup>

---

<sup>30</sup> Cf. Vint Cerf, Growing Up in a Digital World (address given at the Global Internet Summit 2000), <<http://www.govtech.net/magazine/visions/may00visions/digitalworld/digitalworld.phtml>> (imagining the Internet-equipped refrigerator, but assuming that one would manually scan a milk carton's bar code when putting it in the fridge); cp. John C. Dvorak, Smart Homes, Dumb Ideas, PC Magazine (June 26, 2000), available at <<http://www.shed.com/digests/digests2000/06-30-00.txt>>.

<sup>31</sup> See Jack Uldrich, Now You See It . . . , Advantage (Feb. 2004), <[www.fmi.org/advantage/issues/022004/pdfs/pub/nowyouseeit.pdf](http://www.fmi.org/advantage/issues/022004/pdfs/pub/nowyouseeit.pdf)> (describing use of nanotechnology to detect milk spoilage).

<sup>32</sup> See Barnaby J. Feder and Tom Zeller Jr., Identity Badge Worn Under Skin Approved for Use in Health Care, N.Y. Times (Oct. 14, 2004), <<http://www.nytimes.com/2004/10/14/technology/14implant.html>>.

<sup>33</sup> See Press Release: 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), <[http://biz.yahoo.com/bw/040405/55471\\_1.html](http://biz.yahoo.com/bw/040405/55471_1.html)>.

<sup>34</sup> <<http://www.baja-beachclub.com/bajaes/asp/zonavip.aspx>> ("No hace falta llevar monedero. Con sólo pasar por nuestro lector, Baja Beach Club conocerá quién es, y de qué saldo dispone."). English translation is courtesy of <<http://www.infowars.com/print/bb/bajaimplant.htm>>. While not all content on the Infowars site is reliable, the translation seems unexceptional.

<sup>35</sup> See Mexican Officials Get Chipped, Wired News (July 13, 2004), <<http://www.wired.com/news/technology/0,1282,64194,00.html>>; 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, <<http://www.hacer.org/current/Mex064.php>>.

<sup>36</sup> See Julia Scheeres, Tracking Junior With a Microchip, Wired News (Oct. 10, 2003), <<http://www.wired.com/news/technology/0,1282,60771,00.html>>.

This list of actual or proposed uses could go on at some length.<sup>37</sup> Students in an Osaka, Japan elementary school will be getting RFID chips in their schoolbags, name tags or clothing, to be read by readers installed in school entrances and exits.<sup>38</sup> More than 50 million pets have RFID tags.<sup>39</sup>

Governments are not lagging in thinking up RFID implementations. I've mentioned the Defense Department's push for RFID in procurement; the General Services Administration is said to have mandated use of RFID to help it manage information on the buildings, fleets of cars, and other products it oversees.<sup>40</sup> The FDA is moving ahead with plans eventually to tag every package of prescription drugs sold in the US with a unique serial number on an RFID tag, and to use that unique identifier to tie every package to its complete manufacturing and dispensing history, as a guarantee that the drug is what its package holds it out to be and is being sold in authorized channels.<sup>41</sup>

Both the European and Japanese central banks have discussed incorporating RFID tags in currency.<sup>42</sup> The U.S. government is said to have expressed interest as well.<sup>43</sup> The nominal goal here is to make counterfeiting more difficult, as well as perhaps keeping track of money laundering and black-market transactions.

Most alarmingly, perhaps, governments have begun to embed RFID in identification documents. A committee of the International Civil Aviation Organization has approved a recommendation that all passports and other travel documents store electronic data on "contact-

---

<sup>37</sup> 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 News (Mar. 19, 2004), <<http://www.wired.com/news/medtech/0,1286,62723,00.html>>.

<sup>38</sup> Jo Best, Japan: Schoolkids to be tagged with RFID chips, CNETAsia (July 12, 2004), <<http://asia.cnet.com/news/systems/0,39037054,39186467,00.htm>>.

<sup>39</sup> Cathy Booth-Thomas, The See-It-All Chip, Time.com (Sept. 22, 2003), <<http://www.time.com/time/globalbusiness/article/0,9171,1101030922-485764,00.html>>.

<sup>40</sup> See RFID Streamlines Processes, Saves Tax Dollars, <[http://www.sun.com/br/government\\_1216/feature\\_rfid.html](http://www.sun.com/br/government_1216/feature_rfid.html)>.

<sup>41</sup> See U.S. Food & Drug Administration, COMBATING COUNTERFEIT DRUGS § D.1.e (Feb. 2004), <[http://www.fda.gov/oc/initiatives/counterfeit/report02\\_04.html#radiofrequency](http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html#radiofrequency)>.

<sup>42</sup> 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/](http://www.theregister.co.uk/2003/07/30/japan_yens_for_rfid_chips/)> (Japan); Winston Chai, Radio ID chips may track banknotes, News.com (May 22, 2003), <<http://news.com.com/2100-1017-1009155.html>> (EU); 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 Journal (Aug. 4, 2003) (such reports are "wildly premature").

<sup>43</sup> See RFID Streamlines Processes, Saves Tax Dollars, <[http://www.sun.com/br/government\\_1216/feature\\_rfid.html](http://www.sun.com/br/government_1216/feature_rfid.html)>.

less integrated circuit” chips (which is to say, RFID technology or a close relation).<sup>44</sup> The United States, it appears, is moving quickly to implement that recommendation: the State Department expects newly issued U.S. passports to have RFID embedded by the end of 2005.<sup>45</sup> The U.S. Department of Homeland Security is currently equipping trusted travelers crossing the Canadian border with RFID-enabled identification cards, to be read by readers in special lanes at border crossing stations.<sup>46</sup> The state of Virginia is exploring proposals for RFID-equipped driver’s licenses.<sup>47</sup>

## II.

Privacy activists have raised alarms over RFID technology. Persons carrying RFID-enabled goods or documents, they point 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,<sup>48</sup> the possibilities for surveillance once a tire rolling down a highway starts broadcasting its unique ID number are plain. The privacy ramifications of tags in currency are similarly apparent.<sup>49</sup> (Some reports indicate that tags for currency would have a read range of only a few millimeters, so that information seekers couldn’t identify currency from a distance, but details are hard to come by; the tag generally discussed in this connection is

---

<sup>44</sup> See Biometric Technology on Machine Readable Travel Documents — The ICAO Blueprint (May 11, 2003), <[http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp004\\_en.pdf](http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp004_en.pdf)>; see also Privacy International et al., An Open Letter to the ICAO (Mar. 30, 2004), <<http://www.privacyinternational.org/issues/terrorism/rpt/icaoletter.pdf>>. On contactless integrated circuit technology, see generally Michael Hegenbarth, “Contactless” standardization — A Key Issue for Interoperable e-ID Applications (Oct. 10, 2003), <[http://www.itsc.org.sg/events/cpita\\_seminar\\_oct03/Michael\\_Hegenbarth\\_Singapore\\_Seminar3a10prints.pdf](http://www.itsc.org.sg/events/cpita_seminar_oct03/Michael_Hegenbarth_Singapore_Seminar3a10prints.pdf)>.

<sup>45</sup> See Edward Hasbrouck, Time to get a new USA passport, *The Practical Nomad* (Oct. 14, 2004), <<http://hasbrouck.org/blog/archives/000433.html>>; Wilson P. Dizard III, Smart passport field narrows to four, *Government Computer News* (Oct. 18, 2004), <[http://gcn.com/vol11\\_no1/daily-updates/27620-1.html](http://gcn.com/vol11_no1/daily-updates/27620-1.html)>. Passports are already RFID-equipped in Malaysia and Myanmar. Singapore is implementing that technology, see Raghu Das, Smart Labels 2002 Conference Review (Oct. 2, 2002), <<http://www.rfid-handbook.de/forum/read.php?f=10&i=12&t=12>>, and Nigeria has contracted to do the same, <<http://www.idtechex.com/sla29s.html>>.

<sup>46</sup> See Intermec, Life in the Fast Lane: RFID Powers Border Crossing Program, <[http://epsfiles.intermec.com/eps\\_files/eps\\_cs/NEXUS\\_cs\\_web.pdf](http://epsfiles.intermec.com/eps_files/eps_cs/NEXUS_cs_web.pdf)>. In addition, the U.S. Department of Transportation is experimenting with customs seals incorporating RFID on cargo containers. See E-Seals Smooth Border Crossings, *RFID Journal* (Sept. 3, 2002), <<http://www.rfidjournal.com/article/articleview/62/1/1>>.

<sup>47</sup> Mark Baard, RFID Driver's Licenses Debated (Oct. 6, 2004), <<http://www.wired.com/news/privacy/0,1848,65243,00.html>>.

<sup>48</sup> Cf. *Nat'l Tire Dealers & Retreaders Ass'n v. Brinegar*, 491 F.2d 31 (D.C. Cir. 1974) (wrestling with the question how to ensure that a tire’s safety information stays available to the consumer once the tire is retreaded).

<sup>49</sup> See Ari Juels & Ravikanth Pappu, Squealing Euros: Privacy Protection in RFID-Enabled Banknotes, in *Financial Cryptography '03* (R. Wright ed. 2003), available at <<http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/squealing-euros/SquealingEuros.pdf>>.

Hitachi's mu chip, which is said to have a read range of about a foot.<sup>50</sup> Even less obviously problematic uses, activists urge, may jeopardize consumer privacy and threaten civil liberties.<sup>51</sup>

These privacy-based objections have claimed considerable attention. Both public-interest groups<sup>52</sup> and academics<sup>53</sup> have begun focusing on RFID privacy issues. The U.S. Federal Trade Commission has held a workshop exploring the consumer privacy concerns RFID raises.<sup>54</sup>

It may be that we will never see extensive use of RFID in consumer goods, documents or credentials. Most of the RFID implementations I discussed in the previous section are still on the drawing board; we don't yet know which ones will actually be rolled out. RFID tagging of pallets and cases of consumer packaged goods seems to have unstoppable momentum. The move to embed RFID in U.S. passports has distressingly strong force.<sup>55</sup> We can confidently expect RFID tags on prescription drug bottles, airline baggage,<sup>56</sup> and cattle. The business case for RFID tags on individual consumer items more generally, though, seems equivocal.

To begin with, it's not clear whether the cost of RFID tags will drop sufficiently. Industry sources have suggested that we're unlikely to see widespread distribution of item-level tags unless the price per tag drops below five cents, and unlikely to see tags on really cheap consumer items -- say, boxes of cereal and bars of soap -- unless the price per tag drops to below a penny.<sup>57</sup> It's hardly clear that those prices are feasible. The cost of even the least expensive

---

<sup>50</sup> See Hitachi Unveils Smallest RFID Chip, RFID Journal (Mar. 14, 2003), <<http://www.rfidjournal.com/article/view/337/1/1/>>.

<sup>51</sup> See CASPIAN et al., Position Statement on the Use of RFID on Consumer Products 1, available at <<http://privacyrights.org/ar/RFIDposition.htm>>.

<sup>52</sup> A recent position statement on RFID was issued by eight U.S. public interest groups, including such major players as the ACLU and the Electronic Frontier Foundation, and endorsed by others. See id.

<sup>53</sup> See, e.g., Helen Nissenbaum, Privacy as Contextual Integrity, 79 Wash. L. Rev. 119 (2004); Jerry Kang & Dana Cuff, Pervasive Computing: Embedding the Public Sphere, <[http://www.ipercs.ucla.edu/kang\\_cuff\\_embedding\\_v11.pdf](http://www.ipercs.ucla.edu/kang_cuff_embedding_v11.pdf)>.

<sup>54</sup> U.S. Federal Trade Commission, Radio Frequency Identification: Applications and Implications for Consumers, <<http://www.ftc.gov/bcp/workshops/rfid/>>.

<sup>55</sup> See supra note 45 and accompanying text.

<sup>56</sup> See Barnaby J. Feder, Delta to Invest In Radio Tags For Luggage At Airports, New York Times, July 1, 2004, at C4.

<sup>57</sup> Smart Labels Analyst, Progress with Item-Level RFID Special Report (Feb. 2004), <<http://www.idtechex.com/pdfs/en/L6931K9077.pdf>> [hereafter, Progress with Item-Level RFID Special Report]. To make a tag for less than a penny, you'd 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. That's still a long way away.

tag today is more than ten cents by some accounts, and forty cents by others.<sup>58</sup> Getting the price down won't be easy. As one analyst explained the problem:

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.<sup>59</sup>

Others, however, urge that the five-cent chip is feasible with economies of scale.<sup>60</sup>

Even with sufficiently inexpensive tags, 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%.<sup>61</sup> 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.<sup>62</sup> It's important to remember that 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.<sup>63</sup> If item-level tagging is to justify its costs, it will have to be markedly more convenient and more reliable than lower-tech approaches.

---

<sup>58</sup> See Allen Friedman, Predictions amid the Hype: Assessing the Risks of Retail RFID and Privacy (Jan. 2, 2004), <[www.sccs.swarthmore.edu/users/02/allan/RFID\\_Privacy\\_Hype.doc](http://www.sccs.swarthmore.edu/users/02/allan/RFID_Privacy_Hype.doc)>, at 7-8; see also FTC RFID Workshop, *supra* note 10, at 57 (testimony of Britt Wood, Senior Vice President, Retail Industry Leaders Association) (twenty to forty cents)

<sup>59</sup> FTC RFID Workshop, *supra* note 10, at 249 (testimony of Jim Waldo, Sun Microsystems).

<sup>60</sup> *Id.* at 113 (testimony of William Allen, Marketing Communications Manager, Texas Instruments RFID Systems).

<sup>61</sup> *Id.* at 57-58 (testimony of Britt Wood, Senior Vice President, Retail Industry Leaders Association); see also Danny Bradbury, 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>>.

<sup>62</sup> See FTC RFID Workshop, *supra* note 10, at 250 (testimony of Jim Waldo, Sun Microsystems).

<sup>63</sup> For an excellent 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* n. 58, at 9-15. For a similar thought from another angle, here's 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.

But there is room for doubt on that score. Current adopters are wrestling with the fact that RFID tags are subject to considerable interference from items in the retail environment, such as fluids and metal,<sup>64</sup> not to mention nylon conveyor belts and dense materials like frozen meat and chicken parts.<sup>65</sup> Even in environments that can be optimized for RFID, such as distribution centers receiving arriving pallets, readers today are sometimes unable to read more than 80% of the tags.<sup>66</sup> 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.”<sup>67</sup> It will be more difficult to get satisfactory read rates for RFID tags on the retail store floor, which can’t be optimized for RFID readers the way a distribution center can.<sup>68</sup> Finally, if manufacturers use the same UHF frequency band for item-level tagging that they are now using for pallets and cases, then tags will have to be relatively large, often too large to place conveniently on small consumer items.

All this suggests that while case and pallet level RFID is here to stay, 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.”<sup>69</sup> It’s unlikely that we’ll see much item-level tagging within the next ten years.<sup>70</sup> One analyst has suggested that it’ll be 2017 before we see item-level tagging on products cheaper than ten dollars.<sup>71</sup> At the same time, there are contrary indicators: a major U.S. clothing manufacturer may well have plans to implement item-level tagging in the short term.<sup>72</sup> Further, it’s possible to make too much of the distinction between

---

On my application for unemployment when our RFID project goes over budget.  
<<http://www.frontlinetoday.com/frontline/survey/surveyList.jsp?id=92725>>.

<sup>64</sup> Progress with Item-Level RFID Special Report, *supra* n. 57, at 7. Other frequency bands, moreover, will present their own problems. *Id.*

<sup>65</sup> See David Margulius, The Rush to RFID, *Infoworld* (Apr. 9, 2004), <[http://www.infoworld.com/pdf/special\\_report/2004/15SRrfid.pdf](http://www.infoworld.com/pdf/special_report/2004/15SRrfid.pdf)>, at 38; see also Friedman, *supra* n. 58, at 6-7.

<sup>66</sup> Margulius, *supra* n. 65.

<sup>67</sup> *Id.* (quoting Tig Gilliam, partner, IBM Business Consulting Services).

<sup>68</sup> See Ross Stapleton-Gray, Scanning the Horizon: A Skeptical View of RFIDs on the Shelves (Nov. 13, 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.

<sup>69</sup> Lori Valigra, Smart tags: Shopping will never be the same, *Christian Science Monitor* (Mar. 29, 2001), <<http://search.csmonitor.com/durable/2001/03/29/fp13s1-csm.shtml>> (quoting Steven Van Fleet, program director, International Paper).

<sup>70</sup> See FTC RFID Workshop, *supra* note 10, at 60 (testimony of Britt Wood, Senior Vice President, Retail Industry Leaders Association); see also *id.* at 109 (“the economics behind item-level just don’t make sense right now for retailers to implement”)

<sup>71</sup> See *id.* at 59.

case- and item-level tagging. For large, individually packaged items such as television sets, the case *is* the item. Even there, though, an RFID tag on the cardboard box surrounding the set would likely be discarded once the purchaser got the set home.

It's still hard to predict the ultimate penetration of RFID tags into everyday life. Tags may never become widespread on consumer goods; they may become commonplace in connection with some application I haven't discussed in this paper, such as access badges or credit cards. It may be that all the barriers to item-level tagging of retail goods will be overcome in the next fifteen years. I'll continue in this paper on the assumption that RFID technology will ultimately become widespread, although not necessarily pervasive, in some facets of everyday life. We need to consider, thus, how we should think about that from a privacy standpoint.

### III.

What specific characteristics of RFID give rise to privacy concerns? An initial characteristic is that RFID-equipped goods and documents will blab 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 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.

Now, that's not an *inherent* characteristic of RFID technology: It's easy to imagine RFID tags with sophisticated access controls, which wouldn't release their information unless the reader established through a cryptographic handshake that the tags' programmer had authorized it.<sup>73</sup> For a tag securely to authenticate an authorized reader, say via public key cryptography, would be well beyond the resources of a low cost tag.<sup>74</sup> But one could design a somewhat more simple-minded device designed to talk only to authorized readers, without fancy crypto, by enabling simple password protection and having the tag hold a one-way hash of the password needed to unlock its information. This would at least lessen the number of people able to read data off RFID tags, and it could block the use of tags as persistent identifiers.<sup>75</sup> It's by no means clear that this would provide robust protection; using a simple password scheme like this, the most-often queried passwords would likely soon leak out.<sup>76</sup> But it would be a step in the right direction.

---

<sup>72</sup> See *supra* note 26 and accompanying text.

<sup>73</sup> See Sanjay A. Sarma, Stephen E. Weis, & Daniel W. Engels, RFID Systems, Security & Privacy Implications, at § 4.4 (Nov. 1, 2002), <<http://archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-WH-014.pdf>>; see also Istvan Vajda & Levate Buttyan, Lightweight Authentication Protocols for Low-Cost RFID Tags (Aug. 5, 2003), <[http://www.vs.inf.ethz.ch/events/ubicomp2003sec/papers/secubi03\\_p01.pdf](http://www.vs.inf.ethz.ch/events/ubicomp2003sec/papers/secubi03_p01.pdf)>, and sources cited therein.

<sup>74</sup> Sarma et al, *supra* n. 73, at § 4.3.

<sup>75</sup> *Id.* at § 4.4.

<sup>76</sup> See Email from Prof. Edward Felten, Princeton University, to the author (Oct. 28, 2003) (on file with author).

Other technical answers aim at the ability of RFID tags to supply globally unique identity. A more sophisticated RFID architecture would allow tags to emit not a single, unchanging, unique ID, but a series of random pseudonyms, which could only be understood by authorized verifiers.<sup>77</sup> Alternatively, devices could “deserialize” RFID tags, stripping out the unique identifiers to leave only more generic descriptions. All of these would be plausible approaches toward addressing the privacy threats of simple-minded RFID.

So far at least, though, there’s been no movement by device manufacturers or standards bodies to incorporate these approaches into ordinary RFID tags. That shouldn’t be too surprising. The business case for RFID in the retail supply chain (and indeed in most government applications) 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 can’t make a passive tag smart enough to handle, say, public-key encryption without completely blowing the business case for the foreseeable future. As a result: Expensive special-purpose RFID tags incorporate access controls where a particular implementation calls for it and can justify the expense. Run-of-the-mine inexpensive passive tags, on the other hand, and in particular those currently intended for use in the retail supply chain, do not. They disclose their data promiscuously to anybody with a reader. Absent government mandate, that’s not likely to change.

At this point, a skeptic might raise some practical questions. First, how real is this problem? Some people urge that RFID’s privacy problem is inconsequential, because passive tags have a fairly short read range. Yet this doesn’t seem reassuring. Read ranges need not be all that short; the twenty-meter read range I referred to earlier as a theoretical maximum for passive tags leaves room for substantial surveillance capabilities. Moreover, readers can effectively invade privacy even with even much shorter read ranges. One can embed an RFID reader, invisibly, in floor tiles, or carpeting, or a doorway.<sup>78</sup> A read range of only a few feet is entirely adequate to track people coming through a door.

A further question: The data on a tag is just a string of ones and zeros. How much will it reveal to the third-party listener? One can surely write implementations in which a tag’s data points to an entry in a proprietary, limited-access database; in such a case, the listener can learn the tag’s meaning only if he can buy, barter, or otherwise gain entry to the database. When it comes to ordinary item-level tags on ordinary retail goods, it’s not clear how large a group of actors will have access to the information connected with the tags. The system contemplated by the Auto-ID Center as a standard for RFID use in the retail supply chain, establishing the Object Name Space 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.

---

<sup>77</sup> See Ari Juels, Privacy and Authentication in Low-Cost RFID Tags, <<http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/pt-rfid/pt-rfid.pdf>>; see also Miyako Ohkubo et al., Cryptographic Approach to “Privacy-Friendly” Tags (Nov. 15, 2003), <<http://www.rfidprivacy.org/papers/ntt-rfid-privacy-slides.pdf>> (changing tag data through a randomized hash chain).

<sup>78</sup> CASPIAN et al., *supra* n. 51, at 2.

More recently, though, it's 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.<sup>79</sup> 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 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. Some urge that this will ameliorate any privacy threat.

Still, the meaning of common tag "object classes," identifying the type and model of goods supplied by a given manufacturer, will likely 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's by no means clear that the information associated with tag data will remain closely held. It's at least possible, therefore, that a tag on the shoe you purchase in the near future will tell anyone who asks, as you walk around town, that it's 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're wearing or carrying, and could construct a snapshot profile of you on that basis.

Perhaps more importantly, if the retailer who sells me the shoes records that I am the purchaser of a set of shoes with a particular tag number, and then sells that information to a third party, the buyer can associate that unique tag with me without needing access to the tag database. And even without such access, the unchanging data on the tag can serve as a persistent unique identifier of the person carrying it. Without knowing anything about the meaning of data on particular tags, a person with a reader can 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."

One might object that RFID's privacy threat is lessened because much of the information that readers will collect (such as my shoe style, though not the shoe's serial number) 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, automating the information collection and storage process.<sup>80</sup> Imagine, after all, the movement of automobiles down a highway. There's 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 won't in fact be entered digitally except on particular occasions when it's 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

---

<sup>79</sup> See Stapleton-Gray, *supra* note 68; FTC RFID Workshop, *supra* note 10, at 38 (testimony of Sue Hutchinson, Product Manager, EPCglobal); *id.* at 222-23 (testimony of Christopher Boone, Program Manager, IDC).

<sup>80</sup> 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 (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.")

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's important, because the cheaper it is to collect, store and analyze information, the more information will in fact be collected, stored and analyzed.<sup>81</sup>

Another crucial characteristic of RFID is that its surveillance capability follows the target through space, and reveals to data collectors how the target moves through space. When I first began to think about RFID, I focused on the idea that the technology generates information relating to subjects' "real-space" existence. But that's not quite it; after all, nearly all information that a data collector might collect about a person, using any technology, relates to his real-space existence. RFID is new in part because it allows observers to learn a particular thing about my real-space existence that other technologies don't -- and that's *where* I am physically. It's thus, quite directly, a surveillance technology. And there's more: 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 wouldn't recognize her, and that can take actions based on that information.

Here, the skeptic will argue that we need not fear geographic tracking absent a geographically pervasive reader network, and that nobody is likely to put such a network in place. Yet 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. At that point, any particular set of readers need not be pervasive.<sup>82</sup>

Before assessing RFID's privacy threat, finally, we need to note a third characteristic: While strangers can collect RFID data from tags on goods or documents in my possession, that data isn't *necessarily* linked to my name or other personally identifying information. 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 credit-card purchase information.<sup>83</sup> RFID tag information, by contrast, while attached to the geographic location or the physical person of the target, is not necessarily 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.

---

<sup>81</sup> I owe this articulation to Lee Tien.

<sup>82</sup> 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 tracked without placing RFID readers every few feet. They need only be positioned at the entrance and exit ramps." CASPIAN et al., *supra* n. 51, at 6.

<sup>83</sup> 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).

That means that we need to articulate two different scenarios for privacy-invasive use of RFID. In Scenario One, some data collector has drawn 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 EPC with my name and other information in its database. Assuming that the tag isn't disabled at 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 info, 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.<sup>84</sup>

That gives rise to three (related and overlapping) privacy threats. The first is profiling. A reader network can cheaply and seamlessly collect RFID information from my belongings and documents, and easily add it to my profile. When an entity reads information from my tags, it will be able to add to the profile associated with my name any new characteristics associated with that RFID information (as well as the unique tag numbers themselves). This may facilitate more robust and pervasive profiling, incorporating new data signaled by tags on consumers' portable possessions, clothing, vehicles, money, and identification documents.

The second is surveillance. In Scenario One, the devices attached to the reader network will know who the person carrying the tags is. The fact that RFID situates its data subjects in space means that the ability to link RFID tags to names transforms a reader network into a Panopticon geolocator. If we imagine a world in which most people carry tags easily linked to their names (an RFID-equipped drivers license would more than satisfy this criterion), then 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 third is the threat Ravi Pappu describes as the "action threat."<sup>85</sup> After reading RFID tag information when I enter a geographic space, and associating that information with my profile and thus my name, people or devices associated with the reader network can take actions regarding me (ranging from further surveillance and arrest on the one hand, to displaying targeted ads on the other) based on their knowledge of who I am and what I'm like.

The threats in this scenario rely on the fact that the listener knows something about the target *beyond* the information available wirelessly from the tags. The listener is able to connect a tag I carry to my personally identifying information by virtue of the fact that it has collected information about me on some separate occasion, either directly from me, or from some third party who got the information from me (or from some third party who bought the information from some third party who bought the information from some third party who . . . ). I need not

---

<sup>84</sup> 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, back 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 Weinberg, *supra* n. 83, 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.

<sup>85</sup> Ravi Pappu, Privacy and Security in the EPC Network, <<http://www.rfidprivacy.org/papers/pappu.pdf>>.

worry about Scenario One threats from strangers who know nothing about me other than what they can pull from my tags. How much protection does this provide? 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. 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 an important way to limit Scenario One threats.<sup>86</sup>

In Scenario Two, the listener cannot make a connection between the target's RFID data and her name or other personally identifying information. This largely eliminates the profiling and surveillance threats. 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 him to particular goods the seller thinks may be of interest, offering him differential rates, imposing obstacles to his admission to a mall.<sup>87</sup> Moreover, as I've mentioned, the tag numbers can nonetheless serve as unique and semi-persistent identifiers.<sup>88</sup> Any listener 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 given unique tag numbers). This information collection over time can inform the actions I've just described. Moreover, once those dossiers exist, they may be linked to a person's name at a later point, dropping us back into Scenario One.

#### IV.

This discussion indicates that deploying RFID tags with the characteristics I've described may present a substantial privacy threat — and at this point I think it's necessary to devote at least a word or two to why that's a problem, and why we should care. I won't 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 while still capturing our intuitions.<sup>89</sup> But a key aspect of privacy, I'll 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

---

<sup>86</sup> See *infra* notes **Error! Bookmark not defined.-Error! Bookmark not defined.** & accompanying text.

<sup>87</sup> See Kang & Cuff, *supra* n. 53.

<sup>88</sup> I'll describe them here as semi-persistent, since, after all, if a tag is attached to a retail good I'm carrying, I may end up carrying or wearing the good only some of the time.

<sup>89</sup> Robert C. Post, Three Concepts of Privacy, 89 *Geo. L.J.* 2087, 2087 (2001).

others, and how those others will safeguard the information we have disclosed.<sup>90</sup> We create concentric circles of intimacy by disclosing more (or more sensitive) things to people we're closer to, and fewer to others.<sup>91</sup>

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'll be met with disapproval or ill-will from a larger society.<sup>92</sup> 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's something I'd 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.<sup>93</sup>

The profiling, surveillance and action threats posed by privacy-invasive RFID implementations put these values in jeopardy. By promiscuously broadcasting a wide range of information about me to all comers and facilitating the creation of a large-scale profile possibly tied to my name, they deny my autonomy to decide for myself to whom I'll disclose that information. (Again, that remains the case even where particular individual elements of the profile are visually available to strangers in public places; the danger lies in important part in the cheap and easy digital aggregation of all of the pieces of the puzzle that describes me.) By locating me in space, impressing my digital profile on my physical body, privacy-invasive RFID implementations magnify that privacy threat. By allowing strangers to take actions regarding me based on my constellation of tags, they further suppress my ability to make my own choices in a zone of "relative insulation."<sup>94</sup>

## V.

The discussion so far, I hope, has pointed the reader toward two points. First, it would be desirable to design RFID systems so that they don't generate the privacy threats I've described.

---

<sup>90</sup> See Nissenbaum, *supra* n. 53. 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).

<sup>91</sup> See Charles Fried, *Privacy*, 77 *Yale L.J.* 475, 482-86 (1968); James Rachels, *Why Privacy is Important*, in *Philosophical Dimensions of Privacy* 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>>.

<sup>92</sup> See Reiman, *supra* n. 80, at 35-36; Nissenbaum, *supra* n. 53, at 148-49; Fried, *supra* n. 91, at 483-84.

<sup>93</sup> The turns of phrase are from Reiman, *supra* n. 80, at 39. See also 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.").

<sup>94</sup> The phrase is from Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 *Stan. L. Rev.* 1373, 1424 (2000).

Second, if we fail to protect privacy through good technical design, we may need to address the privacy threat through some sort of restraint on information use and sharing.

We have time before any comprehensive set of restraints may be necessary. While we're seeing an extensive and continuing rollout of RFID technology in the retail supply chain, nearly all of that rollout is directed towards cases and pallets. Tags on cases and pallets don't present any significant privacy threat. The main 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.<sup>95</sup> While the evidence is equivocal,<sup>96</sup> it appears that widespread deployment of item-level tags is likely at least a decade away. We have, therefore, some breathing room.

It would be a mistake, on the other hand, to resolve to take no action until item-level tagging systems are fully deployed and consumers have already taken a substantial privacy hit. 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. Further, 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. In addressing RFID's privacy impacts, therefore, we need to walk the thin line between acting too quickly – imposing uninformed policies because we don't yet have a good understanding of what the technology and the marketplace will do -- and acting too slowly, allowing abuses as the sand disappears from beneath our feet.

What answers do we have? 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) has stepped forward with its own approach to privacy protection; it has endorsed the "kill command." Under EPCglobal's first-generation specifications, inexpensive passive tags would be designed to respond to a password-protected command directing the tag's integrated circuit to disable itself. Retailers thus could choose to give consumers the option to have RFID tags on their purchases disabled before they left the store.<sup>97</sup>

---

<sup>95</sup> See Pappu, *supra* n. 85. It's 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* n. 51, 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 (Aug. 22, 2003), <[http://news.com.com/2100-1008\\_3-5067253.html](http://news.com.com/2100-1008_3-5067253.html)>; Howard Wolinsky, P&G, Wal-Mart store did secret test of RFID, Chicago Sun-Times (Nov. 9, 2003), <<http://www.suntimes.com/output/lifestyles/cst-nws-spy09.html>>, but I doubt that RFID is the most important threat there.

<sup>96</sup> See *supra* n. 26 & accompanying text.

<sup>97</sup> The kill functionality is also included in the second-generation protocol specification recently submitted to EPCglobal by thirteen major RFID vendors. See Mark Roberti, 13 Vendors Submit EPC Proposal, RFID Journal (Apr. 20, 2004), <<http://www.rfidjournal.com/article/articleview/893/1/1/>>.

It's not clear to what extent major manufacturers of retail goods (who will be the firms actually purchasing and affixing tags in the retail sales chain) are interested in this kill functionality. According to one source, those users are split. Some are willing to enable killable tags, as an option for consumers; others, such as Nestle, are not. Those others are unwilling to give up the potential functionality of tags that continue to operate past the point of sale (facilitating returns, and the like), and believe that privacy advocates represent a minority who in the end will be unable to stop the technology's rollout.<sup>98</sup>

There's appeal to the "kill command." The option of killing retail tags at point of sale recognizes the different tradeoffs the technology presents at different points in the retail-good 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 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 she sees benefit in that course.

EPCglobal's approach, however, has at least one important flaw: It seems unlikely to do a very good job of actually keeping live tags off the streets. Not all manufacturers are enthusiastic about enabling the kill capability. Retailers are unlikely to want to incur the additional expense. 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'll be receiving, uninvited, on their consumer packaged goods.<sup>99</sup> 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's 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. As scholars have often noted, consumers tend to underestimate the incremental impact on their privacy of allowing just one more set of small disclosures, in part because they're not fully aware of the degree to which any given disclosure can become part of an aggregate, data-mined profile.<sup>100</sup> 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 unsophisticated 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.

So we're back to the question of what sort of legal restraints on information use and sharing might protect against the most egregious threats posed by RFID in the retail sales chain. In other privacy contexts, it's useful to draw the content of legal restraints on information use and sharing from what are commonly described as Fair Information Practice principles. The

---

<sup>98</sup> Smart Labels Analyst, This month's summary (April 2004), at 4-5, <<http://www.idtechex.com/sal39s.html>>.

<sup>99</sup> See Stapleton-Gray, *supra* n. 68.

<sup>100</sup> 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).

Federal Trade Commission's 1998 *Privacy Online: A Report to Congress*)<sup>101</sup> identifies five such core principles, which I'll paraphrase here: (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.<sup>102</sup> Principles like these, though only sporadically reflected in U.S. law, play an important role in U.S. as well as European information privacy thinking.

At least at the outset, fair information practices seem remarkably ill-suited to data collection systems like simple RFID. 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.<sup>103</sup> Fair information practices work best in systems with clearly identified data collectors, who have the information in the first place 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. They work much less well in systems in which devices blab information indiscriminately, so that there's no way to identify a class of information collectors who can be made subject to the rules.<sup>104</sup>

This very incongruity, though, suggests two useful approaches to RFID regulation. The first is to focus on the data regarding which Fair Information Practice principles work best: the personal identifying information that must be linked to tag data to generate a Scenario One privacy threat. As I noted earlier in this paper, the worst RFID privacy threats come when tag data can be linked to an individual's name or other personal identifying information.<sup>105</sup> Fair information practices could be used to address that linkage. A regulator, or a set of industry best

---

<sup>101</sup> U.S. Federal Trade Commission, *Privacy Online: A Report to Congress* (1998), <<http://www.ftc.gov/reports/privacy3/>>.

<sup>102</sup> See [id.](http://www.ftc.gov/reports/privacy3/fairinfo.htm#Fair%20Information%20Practice%20Principles) at § III.A, <<http://www.ftc.gov/reports/privacy3/fairinfo.htm#Fair%20Information%20Practice%20Principles>>; see also FTC RFID Workshop, *supra* note 10, at 275-76 (testimony of Cedric Laurant, Policy Counsel, Electronic Privacy Information Center).

<sup>103</sup> See Pamela Samuelson, *Sensor Networks & Privacy*, presentation given at Conference on Securing Privacy in the Internet Age, Stanford Law School, March 13, 2004, <<http://www.sims.berkeley.edu/~pam/papers/Stanford%20cybpriv.ppt>>, at 8.

<sup>104</sup> On the other hand, this hasn't stopped Portugal's National Data Protection Commission from ruling that RFID data collection is subject to that nation's data privacy laws. See Portuguese Commission Rules RFID Use Subject to Country's Data Protection Law, *Telecommunications Monitor* (Jan. 22, 2004). See also Simson Garfinkel, *Adopting Fair Information Practices to Low Cost RFID Systems* (2002), <[http://www.simson.net/clips/academic/2002\\_Ubicomp\\_RFID.pdf](http://www.simson.net/clips/academic/2002_Ubicomp_RFID.pdf)>.

<sup>105</sup> See *supra* text accompanying notes 84-86.

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.<sup>106</sup>

The second approach would impose restrictions on tag data collection to minimize the respects in which RFID makes Fair Information Practice principles problematic. One could, for example, prohibit the use of tag readers except where individuals have been warned that they are present; one could require that readers emit a tone or light, or some other easily recognizable indicator, when they draw information from RFID tags.<sup>107</sup>

Neither of these, though, individually or together, address all of the dangers presented when citizens and consumers are walking around with live, unsophisticated, serialized tags. We should also think about simpler answers. With respect to government use, for example, some of the appropriate answers are stark: Unsophisticated RFID tags should not be in drivers' licenses. Indeed, given the dangers of government surveillance, even sophisticated RFID tags should not be in drivers' licenses.<sup>108</sup>

With respect to commercial RFID, there seem to be simpler and more effective alternatives to EPCglobal's kill functionality. I can see no good reason not to require, as the Electronic Privacy Information Center has recommended, that RFID tags attached to individual items in the retail sales chain be clearly labeled and easily removable.<sup>109</sup> That shouldn't pose an insuperable barrier for industry; EPCglobal's own "best practice" guidelines for RFID tags on consumer products "anticipate[] that for most products," tags will be "part of disposable packaging or . . . otherwise discardable."<sup>110</sup>

---

<sup>106</sup> All of these suggestions can be found in the Electronic Privacy Information Center's proposed guidelines for commercial use of RFID. See Comments of the Electronic Privacy Information Center to the Federal Trade Commission (July 9, 2004), in connection with the FTC Workshop on Radio Frequency Identification Applications and Implications for Consumers, <<http://www.epic.org/privacy/rfid/ftc-comts-070904.pdf>>, at 17-18. See also FTC RFID Workshop, *supra* note 10, at 205 (testimony of John Parkinson, Vice President and Chief Technologist, 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").

<sup>107</sup> These restrictions too can be found in EPIC's guidelines. See *id.* at 17.

<sup>108</sup> See *supra* text following note 84; Testimony Before the Virginia Legislature on House Joint Resolution 162, Considering the Creation of Smart Driver's Licenses (Chris Calabrese, ACLU) (Oct. 6, 2004), <<http://www.aclu.org/Privacy/Privacy.cfm?ID=16658&c=39>>. See also Edward Hasbrouck, RFID passport data won't be encrypted, *The Practical Nomad* (Oct. 15, 2004) <<http://hasbrouck.org/blog/archives/000434.html>>; Bruce Schneier, Passport radio chips send too many signals, *International Herald Tribune* (Oct. 4, 2004), <<http://www.ihf.com/articles/541711.html>>.

<sup>109</sup> *Id.* at 14; see also FTC RFID Workshop, *supra* note 10, at 190 (testimony of Beth Givens, Director, Privacy Rights Clearinghouse). This rule might not apply if a tag were sophisticated enough to implement privacy protection, or if it carried only a generic (not globally unique) identifier.

<sup>110</sup> EPCGlobal, Guidelines on EPC for Consumer Products, <[http://www.epcglobalinc.org/public\\_policy/public\\_policy\\_guidelines.html](http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html)> (last modified Sept. 13, 2004).

This approach, it is true, would force consumers to choose between privacy protection and post-sale tag functionality. If a consumer discarded a tag, she wouldn't get the benefit of a retailer's use of RFID to facilitate returns (a consumer, some have suggested, might be able to return an item without proof-of-purchase if the item retained its tag and the store had associated the sale price and the buyer's name with the tag ID in its database at point of sale). Similarly, if consumers discard tags, recycling centers will not be able to rely on EPCs to categorize recycled items. Consumer items such as stoves and washing machines will not be able to read tag information to get cooking or washing instructions.<sup>111</sup> This nonetheless strikes me as the best approach on balance. Consumers will be able to retain tags when they choose to.<sup>112</sup> Manufacturers will remain free, if they choose, to incorporate information more permanently into consumer goods via a non-wireless bar code, or a generic tag not carrying a globally unique identifier. I suspect that the cool and valuable post-sale uses of unsophisticated EPC tags will be few (in part because manufacturers' reluctance to expose tag data to the world via the ONS will make it harder for third parties to offer post-sale functionality). The privacy-invasive uses of EPCs once goods are sold, by contrast, will be many -- that's the direction that economic incentives push in. Allowing consumers easily to opt out, simply by tearing off RFID tags and dropping them in the trash, makes sense.

## CONCLUSION

It's hard to predict the ultimate penetration of RFID tags. In this paper, I assume that RFID technology will ultimately become widespread, although not necessarily pervasive, in some facets of everyday life.

A variety of planned RFID implementations, including item-level tagging of consumer goods, give rise to serious privacy concerns. If an ordinary citizen is carrying items or documents equipped with RFID tags, then complete strangers can read information from those tags without any current or prior relationship with the person carrying them. That's not a technical inevitability: It's easy to imagine RFID tags with sophisticated access controls, which won't release their information unless the reader establishes through a cryptographic handshake that the tags' programmer has authorized it. But current plans for, and trials of, inexpensive RFID tags don't incorporate that feature, and the business case for pervasive tagging won't accommodate it.

---

<sup>111</sup> These uses are from Ari Juels et al., *The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*, at 3, available at <<http://theory.lcs.mit.edu/~rivest/JuelsRivestSzydlo-TheBlockerTag.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.

<sup>112</sup> For what it's 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.

Moreover, RFID surveillance capability follows the target through space, and reveals to data collectors how the target moves through space. RFID is thus, quite directly, a surveillance technology. 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 wouldn't recognize her, and that can take actions based on that information.

It's important to design sensor systems so that they don't generate the privacy threats I've described. The standards body for RFID in the retail sales chain has endorsed the "kill command," suggesting that at point of sale the consumer would have the option to ask that a tag be disabled. This approach has virtues, but seems unlikely to do an especially good job of actually keeping live tags off the streets. When it comes to RFID tags attached to individual items in the retail sales chain, a variety of approaches might more effectively protect privacy. The simplest would be to require that the tags be clearly labeled and easily removable, so that consumers can easily and uncomplicatedly see to their own privacy protection.