Prepared Statement of

Paula J. Bruening
Staff Counsel
The Center for Democracy & Technology
before
The House Committee On Energy and Commerce
Subcommittee on Commerce, Trade, and Consumer Protection
on
Radio Frequency Identification (RFID) Technology

Wednesday, July 14, 2004

Mr. Chairman and members of the Subcommittee, the Center for Democracy & Technology (CDT) is pleased to have this opportunity to speak to you about both the promise and the possible privacy risks of radio frequency identification (RFID) technology.

CDT is a non-profit, public interest organization dedicated to preserving and promoting democratic values in the digital age. A core CDT goal is to enhance privacy protections for individuals in the development and use of new technologies. We have long advocated the view that privacy considerations are best addressed early in the technology development process, and we applaud the Subcommittee for holding early hearings on this nascent, but potentially revolutionary, technology.

Creative applications of radio frequency identification (RFID) devices hold possibilities for consumers, businesses and government. They can reduce costs in inventory management, improve drug safety, help to reduce error rates and save lives in hospitals, and better track luggage and cargo at airports to increase homeland security.

There are many possible applications of RFID that do not pose major privacy concerns. But to the extent that RFID devices can be linked to personally identifiable information, RFID raises important privacy questions. In an era of widespread collection of data about individuals, RFID heightens concerns about the ability of businesses and government using these technologies to create deep, rich profiles about people and their travels, lifestyles, interests and activities.

In our testimony today, we wish to emphasize six principle points:

- RFID technology poses significant and novel privacy concerns.

- At the same time, well-established principles of fair information practice provide a ready framework to address many of these issues.

- The privacy concerns raised by RFID can be addressed, but they must be handled early. This will require the engagement and commitment of the companies involved. Good work is already being done, but privacy guidelines for RFID must be specific and clear.

- The privacy concerns with the federal government's use of RFID need considerably more attention.

- Technology-neutral baseline privacy legislation could answer many of the basic concerns posed by RFID without creating technology mandates. Legislation aimed specifically at RFID technology is probably undesirable. Companies should not be deploying RFID devices in situations that involve correlation of personally identifiable information until the rules are clear.

- A comprehensive technology assessment is needed at this time. Such an assessment would provide critical information that would help lawmakers, privacy and consumer advocates, technology developers and businesses to avoid serious potential pitfalls.

1. Novel Privacy Issues Raised by RFID

Discount cards, other "customer loyalty cards" and credit cards already collect information about individuals, providing a rich store of information about our likes and dislikes in cars, clothing, travel and many other preferences. The extent to which RFID tags possess the ability to further enhance those profiles by tracking an individual's movements—whether through a store or through the world—will raise new and deeper concerns. The freedom to move freely and without being monitored is basic to the American concept of individual autonomy.

These concerns are further heightened as the wall between government and business collection of information becomes increasingly porous, and as government looks increasingly to commercial databases as a resource for homeland security and law enforcement.

Information gathering using RFID differs from other kinds of data collection in at least three significant ways:

- First, it is **invisible** to consumers: unless the consumer is made aware of the technology, he or she will likely not know that the devices are in use. Data collection occurring with a loyalty card or a bar code involves a visible device that the user can see and touch when the collection takes place. RFID raises the specter of data collection via a device of which the consumer may not even be aware in the sleeve of a blouse or the hem of a pair of trousers.

- Second, the information collection is **passive** with respect to the consumer. A consumer using a credit card actively relinquishes either the card or the account number to a business to make payment for goods or services. In the act of giving the credit card or number, the consumer actively decides to engage in a system that collects certain information about the transaction, not only about the account, but also about the nature of the goods purchased, and when and where the transaction occurred. The consumer is reminded of the event when he receives a statement at the end of the month that specifies when the card was used and what charges were incurred. In contrast, information can be collected by RFID absent any active step on the part of the consumer to turn over the information, and no record of the collection is provided to the consumer.

- The **kind of information** potentially collected using RFID is unique. While we have become somewhat accustomed to the concept of personal profiles that are built on our buying habits, travel activities and demographics, RFID potentially allows much more fine-grained data collection than previously possible. RFID tags can contain globally unique IDs that distinguish a *particular* book from all other copies of that book. As RFID sensors proliferate, the abundance of collection points—and the detail of location data that can be gathered—also increases.

Together, these changes enable data collection and sharing scenarios that are currently impossible. For example, today, the use of “frequent buyer” cards (also known as “customer loyalty cards”) allow stores to keep records of consumer purchases over time, even when payments are made with cash. With RFID, however, it is possible to track not just what items consumers leave the store with, but also where they go with such items and for how long they keep them. If RFID were built into consumer “loyalty cards” it would also be possible to tell not only what you bought but also what you looked at. RFID transfers to the brick and mortar world the type of very specific tracking of interests that is possible online. Without notice, consumers would not necessarily be aware that this kind of tracking was going on.

Similarly, the proliferation of RFID technology raises heightened concerns about data sharing and centralization. There is a strong analogy in this case with our experience with “cookies.” While cookies were originally designed to allow consumers to have a consistent experience within a single website, the spread of the technology eventually gave rise to information from across websites being linked through third-party cookie systems. Similar problems could arise with RFID, because an RIFD reader can typically read any tag. As readers proliferate in stores, libraries, hospitals, and public places, there will be strong incentives for companies to share and link information about the tags they distribute and the tags they read.

The comments of technologists at recent events sponsored by the National Academy of Sciences and Department of Commerce indicate that while the power of this technology is currently limited, developers are working to increase the amount of information the tags can hold, enhance the effectiveness of the readers, lower the cost of the technology, and make the infrastructure far more ubiquitous.

2. Fair Information Practices

RFID implementation must be guided by principles of fair information practice that give consumers control over the collection and use of their personal information.

In 1973, at the beginning of the computer revolution, principles of fair information practices were articulated as guidelines for protecting privacy. These principles form the basis of the Privacy Act of 1974 and similar laws enacted at the state level. They also serve as the foundation of laws enacted at the federal level to address privacy in specific sectors, notably in credit, medical, and financial records. They have been incorporated into industry codes of best practices and form the underpinnings of international agreements on data protection. The principles are intended to give individuals control over their personal information, limit data collection, and place responsibilities on data collectors.

While exact formulations of fair information practices differ, the common elements are relatively standard. They include:

- *Notice:* Information collection and use should be open and transparent.
- *Purpose specification:* Personal data should be relevant to the purposes for which it is collected.
- *Use limitation:* Data should be used only for the purpose for which it was collected.
- *Accuracy:* Personal data should be accurate, complete, and timely.
- *Security:* Personal data should be protected by reasonable security safeguards against risk of loss, unauthorized access, destruction, use, modification or disclosure.
- *Access:* Individuals should have a right to view all information that is collected about them to correct data that is not timely, accurate, relevant or complete.
- *Accountability:* Record keepers should be accountable for complying with fair information practices.

In November of last year, CDT joined with a broad coalition of privacy and civil liberties organizations in calling for the application of fair information practices to RFID.[1] These

[1] The "Position Statement on the Use of RFID on Consumer Products" November 14, 2003 was issued by: Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), Privacy Rights Clearinghouse, American Civil Liberties Union (ACLU), Electronic Frontier Foundation (EFF), Electronic

principles should apply to the gathering of information using RFID and to the handling of that information. They provide a starting point for all ongoing and future efforts to understand and address the RFID privacy issue.

Determining how fair information practices can be applied in a practical, useful and meaningful way will require work on the part of stakeholders.

3. Addressing Privacy at the Outset: Industry Engagement and Best Practices

If companies and government are to successfully and responsibly deploy RFID technology, they need to address upfront the significant trust issues the technology raises. Using RFID in pallets to assist distribution processes and inventory control does not raise major privacy concerns. But as soon as RFID tags are related directly to individual product items, it will be extremely important that consumers clearly understand that the technology is in use, what information is being collected, how it is collected, and how it is used. If consumers are to accept the use of this technology, it is critical that they have assurances that information collected through RFID is managed and used in a responsible fashion.

Experience has shown that when new information collection technologies are deployed, consumers want to know specifics about what and how data about them is being gathered. They want to know upfront from the organization collecting the information, and not through the popular media. It is critical with RFID, as in other emerging technology, that privacy protections are built in at the beginning.

Technology developers and businesses often raise the issue of the cost of building privacy into new technology. CDT would caution that **it is more effective and efficient to begin at the outset of the development process to create a culture of privacy that incorporates sound technical protections for privacy and that establishes the key business and public policy decisions for respecting privacy in RFID use before RFID is deployed, rather than building in privacy after a scandal or controversy erupts publicly**.

Work toward developing principles that would address privacy concerns raised by RFID is ongoing. For example, CDT applauds EPC Global for their work on public policy guidelines that address privacy issues.[2] However, for these principles to be successful in protecting privacy, it is critically important to concretely determine how these principles are applied in practice.

Privacy Information Center (EPIC), Junkbusters, Meyda Online, PrivacyActivism and endorsed by many others including CDT. It is available at http://www.privacyrights.org/ar/RFIDposition.htm.

[2] "Guideline on EPC for Consumer Products" is available at http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html.

For example, notice and public education are often pointed to as key to sound privacy protection for RFID data collection. This is undoubtedly true. But while we may easily agree on this point, it will be extremely important to understand how notice can be *effectively* provided in the RFID environment, in a manner that is consistent and balanced, where information collection is arguably invisible and passive. How to provide notice effectively, and in a manner that is consistent for consumers and presented in a balanced, neutral way, will be a critical challenge.

Similar issues are raised as steps are taken to provide consumers with choice about collection of information through RFID. How do we provide meaningful choice for consumers? How do we make it easily accessible and exercisable in this kind of technology environment? How can we assure that consumer choice has been respected?

4. Government Use of RFID Raises Special Concerns and Requires Special Consideration

Federal, state and local governments have taken a leadership role in the deployment and use of RFID technology. Some governments have used the launch of RFID applications as an opportunity to balance privacy concerns with the use of the technology. For example, the Office of the Information and Privacy Commission of Ontario has released "Guidelines for Using RFID Tags in Ontario Public Libraries."[3] U.S. governments have undertaken little of this important work.

The Department of Defense has been a leader in the RFID field and is engaging in innovative uses of the technology for tracking items within its warehouses.[4] Other federal agencies are following suit with projects outside of the warehouse, such as the Department of Homeland Security's enormous US-VISIT contract.[5] While the government should be encouraged to develop uses of RFID technologies to increase efficiency and cut down on fraud and waste, little or no emphasis has been placed on the privacy concerns attendant to the deployment of the technology. The concerns are particularly acute in government implementation of RFID, as the technology will likely be tied to services that individuals have no option to receive elsewhere.

CDT calls upon the Office of Management and Budget (OMB), General Services Administration (GSA) and National Institute of Standards and Technology (NIST) to develop privacy guidance for agency use of RFID, as they have for electronic authentication technologies. Congress should also explore whether current privacy laws, such as the Privacy Act, Computer Matching and Privacy Protection Act and Section 208

[3] http://www.ipc.on.ca/docs/rfid-lib.pdf

[4] Andrew T. Gilles, "Pentagon: Rough RFID Ride Ahead," Forbes.com, July, 7, 2004, http://www.forbes.com/technology/enterprisetech/2004/07/07/cz_ag_0707beltway.html

[5] Jonathan Krim, "U.S. May Use New ID Cards At Borders," *Washington Post,* June 5. 2004, page E1.

of the E-Government Act, whether these laws adequately cover use of RFID by government agencies.

5. Baseline Privacy Legislation Would Address Many of the Issues Posed by RFID

Despite ongoing public concern about privacy, and despite the fact that privacy issues arise with each new technology that collects personally identifiable information (e.g., cookies, spyware), the United States still lacks baseline privacy legislation that would address privacy concerns raised by the collection of personally identifiable information in new digital media.[6]

In our view, in the absence of such legislation and in the absence of clear, specific industry guidelines, it is unwise for companies to deploy RFID technologies in consumer applications that involve personally identifiable information. Implementing RFID without this guidance raises the risk that it will be necessary to impose rules after the technology has been deployed, when rules may be more cumbersome and less effective, and when it is less likely that technical protections for privacy can be optimally integrated into the technology. It is for this reason that CDT and others have said that RFID should not be deployed at the consumer level in ways that can be linked to personally identifiable information until privacy guidelines are put in place, either by industry, the Congress or state legislators.

CDT believes that it would not be appropriate to enact legislation specially regulating RFID. To enact legislation specifically for RFID would risk technology mandates that are ill-suited to the future evolution of the technology. On the other hand, technology-neutral baseline privacy legislation would ensure that retail and marketing uses of the technology in conjunction with personal information were bounded by fair information practices. Location information, whether generated by cell phones, by mobile computing, or by RFID, also merits stronger privacy protections.[7] These two crucial privacy issues should be addressed in technology-neutral ways.

6. The Need For Technology Assessment

[6] See the testimony of CDT President Jerry Berman before the full Senate Commerce Committee on October 3, 200 at http://www.cdt.org/testimony/001003berman.shtml. His testimony addressed S. 2606, a bill that passed the Committee that year and would have created a baseline standard for privacy on the Internet and allowed the FTC to create regulations for offline privacy in the retail and marketing space.

[7] See the testimony of CDT Executive Director James Dempsey before the Subcommittee on the Constitution of the House Judiciary Committee on September 6, 2000 at http://www.cdt.org/testimony/000906dempsey2.shtml. His testimony addresses H.R. 5018, a bill that passed the Committee that year and would have increased location standards for the use of information by law enforcement.

While specific regulation of RFID technology may be inappropriate, a technology assessment conducted by an expert panel is sorely needed. Such an assessment could be conducted under the auspices of the National Academy of Science, the Federal Trade Commission (FTC), or the National Institute of Standards and Technology (NIST).

Already legislatures are beginning to look at RFID and the privacy concerns the technology raises. Both industry and consumer groups are developing privacy guidelines for use of the technology. But stakeholders on all sides of the debate share a concern about institutionalizing solutions that stifle innovation and have unintended and unwanted consequences for privacy and for RFID technology. Any decision about privacy must be based on sound analysis, the input of all stakeholders, reliable information, and a clear understanding of the technology—both its potential benefits and the risks it raises.

CDT believes that a technology assessment could provide critical information that would help legislators, policy experts, technology developers and businesses to avoid these pitfalls. Technology assessment—an analysis of RFID that explores the technology, how it works, its potential to serve individuals, the vision for the future of the technology, how its use may proliferate and develop and the risks it raises for privacy—could provide the analytical underpinnings to make possible the best possible resolution of privacy concerns. Technology assessment could also surface concerns that are not immediate but that are raised through the establishment of an infrastructure for RFID.

Such an assessment would bring to bear the expertise of technologists, academics, privacy advocates, consumer advocates, manufactures, retailers, security experts and other potential users of RFID technologies. Many of these efforts are already ongoing in public interest organizations and in business research, so that many of the individual pieces of a technology assessment are already in progress. A formal technology assessment would capitalize on these efforts, draw this work together and provide neutral, balanced analysis.

It is important to note that when done well, technology assessment does not arrive at facile solutions. When done fairly, it does not yield simple answers to satisfy a single interest group. Rather, it provides policy options based on the richest, most accurate store of information about the issue possible and the most balanced analysis available. Timeliness is, of course, always a concern when developing technologies are at issue. The online tools at our disposal should make it possible to engage in the assessment exercise in a timely manner that serves both the needs of business for prompt input and the needs of all stakeholders for a chance to bring their concerns to the discussion.

Conclusion

CDT urges Congress to continue to closely monitor the privacy concerns raised by RFID. Business, technologists and consumer advocates must continue to address this issue as the technology and its applications are developed. Additional Congressional hearings would reinforce the need for ongoing work in the private sector to develop and institute best practices for privacy in RFID use. Baseline privacy legislation would help address significant privacy concerns raised by RFID, as well as by other developing technologies. While it is possibly unwise to create RFID specific regulation at this time, we urge Congress to request that the National Academy of Sciences or another neutral, expert body conduct a technology assessment that would provide the technical and policy underpinnings for the best possible legislative solution, when it is timely and appropriate. We look forward to working with the Committee on this critical issue.