RFID

Core-Edge Working Group Meeting, September 28-29, 2004

Natalie Klym
Research Associate, MIT CFP
nklym@comcast.net

2. Introduction

- RFID technology enables contactless identification of tagged objects
- RFID technology has been around for decades, but as cost and size of chips shrink, RFID tags + readers are proliferating
- Potential for billions of nodes, generating huge amounts of data
- New applications leverage the Internet for ID resolution
- The market is currently focused on supply chain applications (driven by DoD and Wal-Mart mandates)
- Consumer apps are on the horizon

3. Key application types

1. Identification & tracking of physical world objects
   - Supply chain objects (inventory)
   - Other “proprietary” objects
     - children
     - prisoners
     - citizens
     - natural resources
     - public landmarks
     - places

The first wave

- All objects have a “virtual presence”
- Tag IDs refer to sources of information about the object
- Based on simple semantics (one-dimensional identifier)
- Object data in the core
- Focus on supply chain applications

2. Near Field Communication (NFC)
   - Combines identification and interconnection technologies for device-to-device communication
   - e.g., mobile phones access content and services

The next wave

- Devices have IDs that can be exchanged for close range communication
- Based on complex semantics (multi-dimensional identifier)

4. Identification & tracking

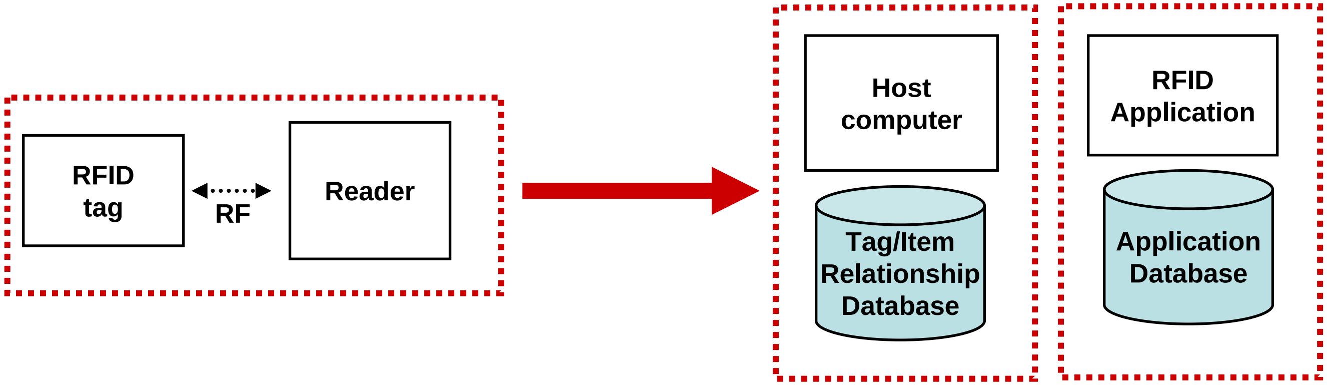
Small tag, big network

- simple semantics – smaller object IDs refer to larger data associated with the object
- intelligence and complexity moves to the core
- minimize size & cost of chip
- serves applications requiring mass production of chips and/or micro tags

5. Identification & tracking

- Technical infrastructure transfers data from tags to IT systems via readers

- Logical infrastructure resolves IDs to associated data



Tag ID → Associated data

6. ID resolution systems

Database field

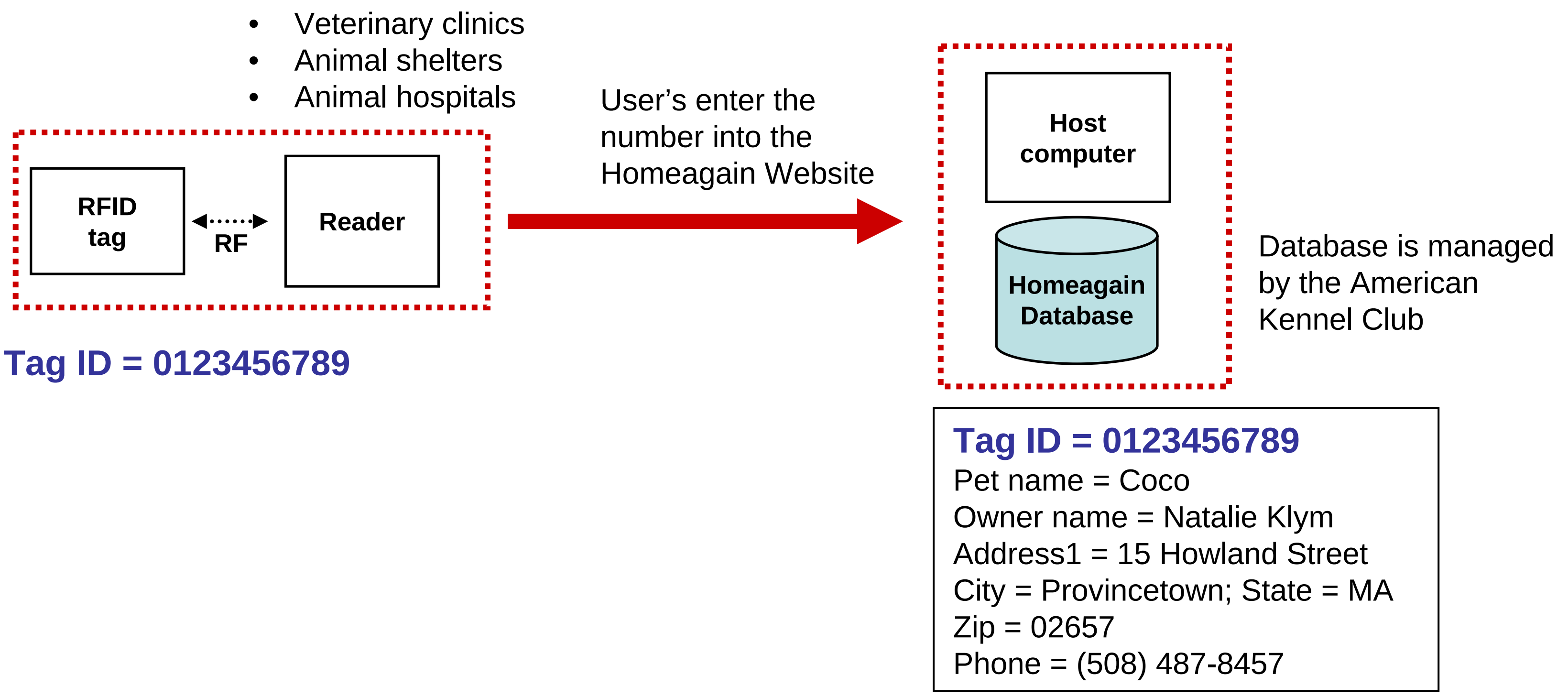
- ID code resolves to a database field in an object’s record
- Appropriate for closed systems, where objects have meaning in a single context
- ID codes are proprietary, and registration is internal
- ID resolution is integral to the database (i.e., not a discrete system)

Pointer (“Internet-of-Things”)

- ID code points to the location of object data on the Internet
- Better for open systems, where objects appear in multiple contexts that must interoperate (e.g., supply chain)
- Multi-context systems require standardized IDs and external (3rd party) registration
- External registry cross-references IDs to multiple (external) sources

7. Homeagain pet tracking

- American Kennel Club Companion Animal Recovery Program
- Pets are tagged and registered
- Tag IDs refer to records in a database
- Database is accessible over the Web by authorized parties
- Tags are read and ID number is manually entered on the Homeagain Web site
- Basic model used for tracking other objects



- Veterinary clinics
- Animal shelters
- Animal hospitals

User’s enter the number into the Homeagain Website

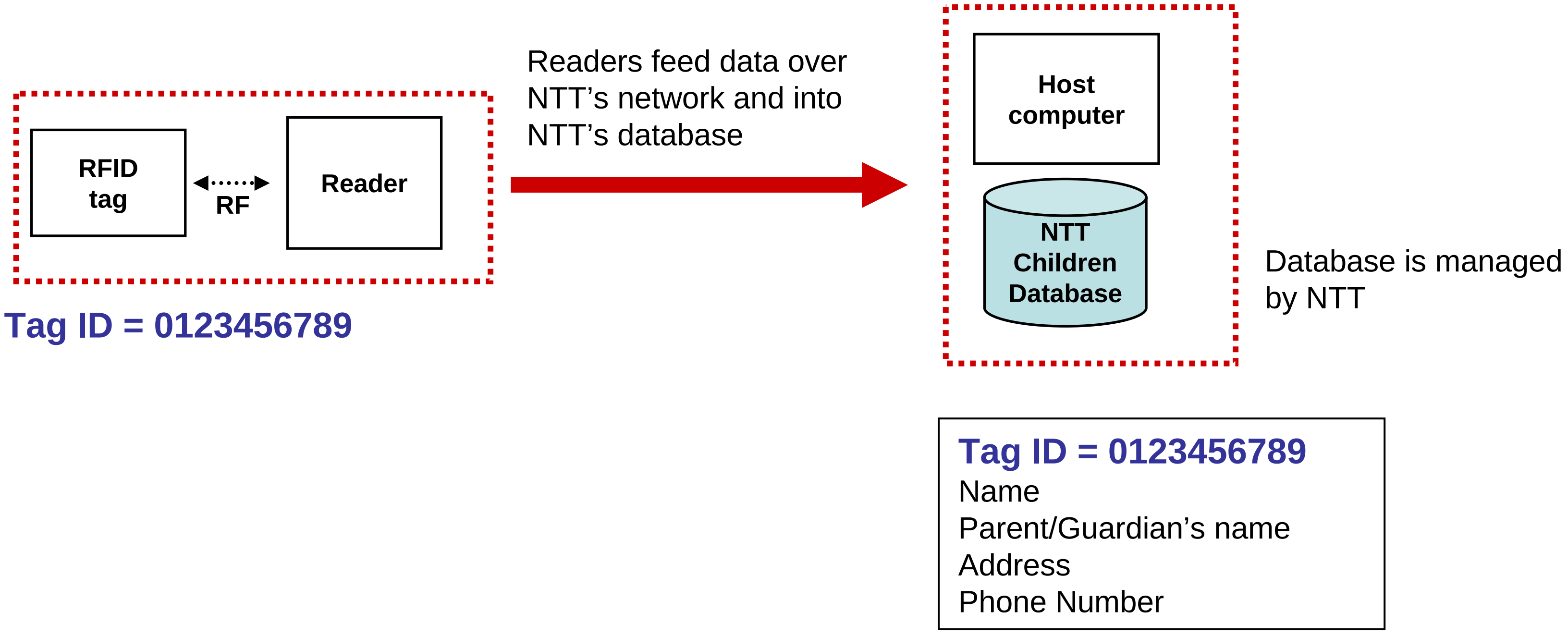
Database is managed by the American Kennel Club

Tag ID = 0123456789

Tag ID = 0123456789
Pet name = Coco
Owner name = Natalie Klym
Address1 = 15 Howland Street
City = Provincetown; State = MA
Zip = 02657
Phone = (508) 487-8457

8. NTT Child tracking

- Child tracking service (real time, fixed reader network)
- Provided by Japan’s NTT Marketing Act Corp. (subsidiary of NTT)
- Children where name tags with RFID tags
- Tag IDs refer to records in a database
- Parents monitor children’s presence online (video cameras are also used)



RFID tag

RF

Reader

Tag ID = 0123456789

Readers feed data over NTT’s network and into NTT’s database

Host computer

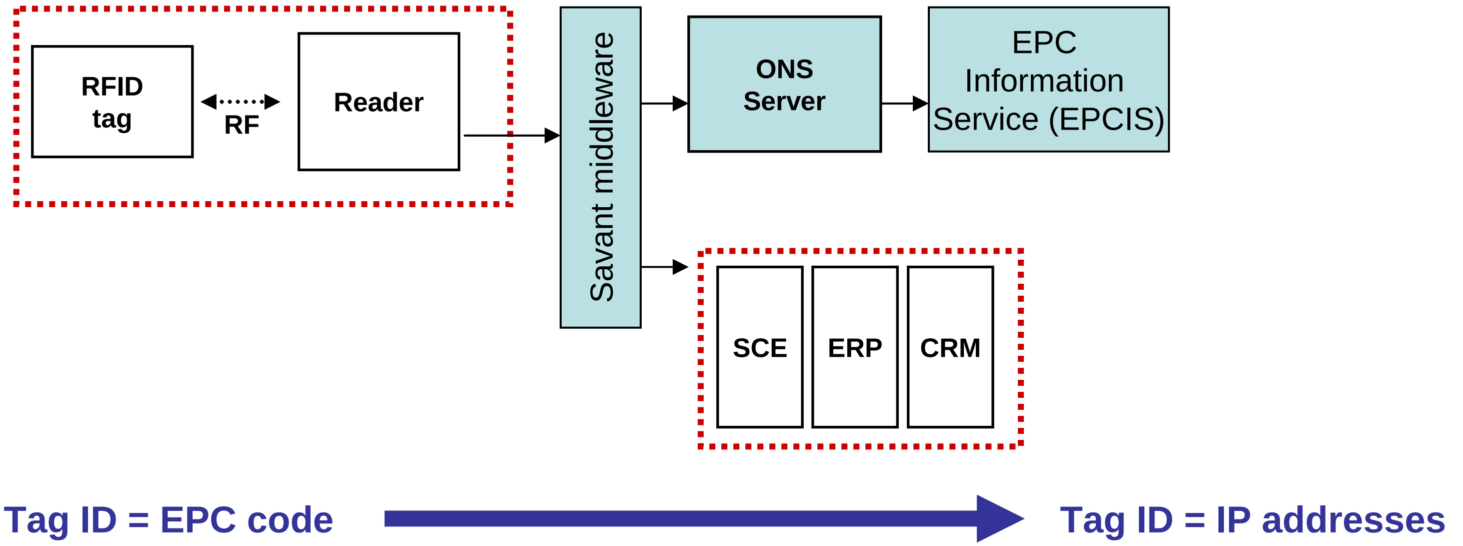
NTT Children Database

Database is managed by NTT

Tag ID = 0123456789
Name
Parent/Guardian’s name
Address
Phone Number

9. The EPC network

- Objects are tagged with standard EPC (Electronic Product Code)
- Savant server acts as a local repository for EPCs and associated information; it connects to internal IT systems and the ONS server
- ONS directory resolves EPC to IP address(es) of object data
- EPC information services converts EPC data into the PML format, enabling interoperability with trading partners
- ID resolution becomes a 3rd party service (could it be owned by someone?)
- “Internet-of-supply-chain-things”



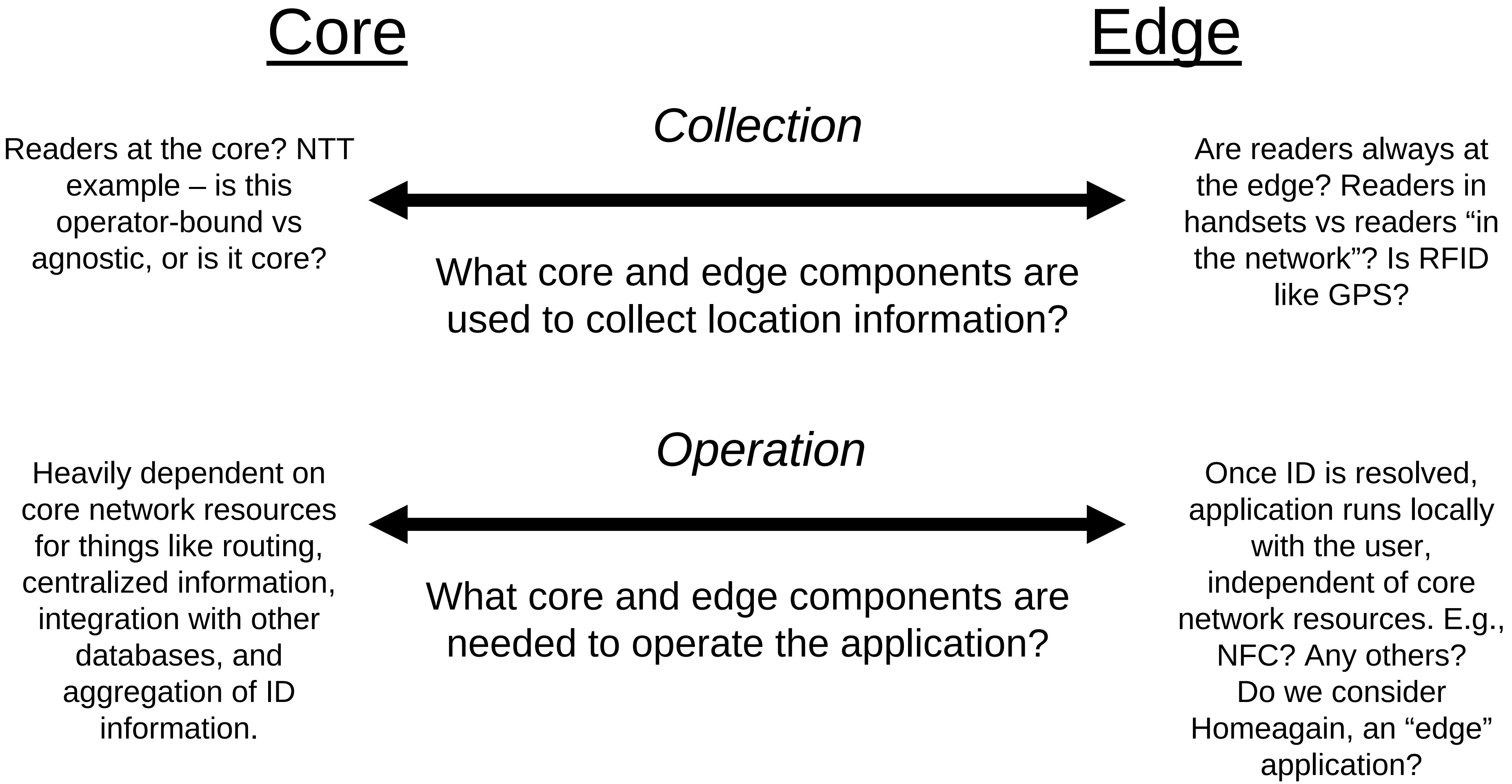
10. Near Field Communication (NFC)

- Next phase of RFID technology
- Very close-range wireless technology for automatic P2P network configuration by touching devices together
- Enables exchange of ID information to establish a connection
- NFC can then bootstrap Bluetooth or Wi-Fi for further data transfer
- Chips contain more intelligence & communicate complex semantics regarding the object
- Chips are more expensive, but relative cost of chip to device is low
- Application examples
  - Content transfer
    - Download music by tapping a device against a poster
    - Display a digital photo on a television
    - Secure payments
    - Access
  - Device-to-device communication
    - Set up communication for other protocols

11. RFID variables – are these all Core-Edge dynamics?

- Technical infrastructure
  - operator agnostic vs operator dependent
    - (e.g., Homeagain, vs NTT child tracking)
  - mobile vs fixed readers
- Logical infrastructure
  - simple vs complex semantics
  - single vs multiple semantic contexts
  - universal IDs vs multiple IDs
  - database record vs IP address
  - direct pointers vs indirect pointer
  - internal vs external registry

12. Can we apply the LBS framework to RFID?



Core

Edge

Collection

Readers at the core? NTT example – is this operator-bound vs agnostic, or is it core?

What core and edge components are used to collect location information?

Are readers always at the edge? Readers in handsets vs readers "in the network"? Is RFID like GPS?

Operation

Heavily dependent on core network resources for things like routing, centralized information, integration with other databases, and aggregation of ID information.

What core and edge components are needed to operate the application?

Once ID is resolved, application runs locally with the user, independent of core network resources. E.g., NFC? Any others? Do we consider Homeagain, an "edge" application?

Extra slides

14. RFID barriers to adoption

- Consumer privacy
  - What happens to product tags when they leave the store?
  - Solutions like “killing tags” may violate DMCA (assuming RFID tags constitute IP)
  - Killing tags may also reduce value of interactive consumer applications (clothes + washing machine, food + fridge, etc.)
  - Who has access to readers
  - Ethics re tagging humans →refs to “Minority Report”, Nazi concentration camps, mark of the beast
- Supply chain security
  - Damaged, removed or vandalized tags
  - Remote interception by hackers
- Abuse of information by firms (anti-competition)
  - Price discrimination among individual customers
  - Price discrimination among geographic markets (violates EU’s single market)
- Standards
  - Tag IDs (competing standards for object codes, e.g. EPC vs ISO)
  - Lack of cooperation among participants (e.g., Intermec demanding royalties)
  - Proprietary tag/reader systems
  - Global frequency standards
- Cost
  - The 5cent tag is still years away
  - Cost sharing among suppliers
  - ROI
- Complexity
  - Tags are application specific
  - Data integration with back-end systems (intra- and inter-firm)
- Data management
  - Data capture – what objects to tag, with what kind of data
  - Data filtering – how to process incoming data

Barry Steinhardt
Director of the Technology and Liberty Program
The American Civil Liberties Union
125 Broad Street, 18th Floor
New York, NY, 10004

Radio Frequency Identification (RFID) Technology: What the Future Holds for Commerce, Security, and the Consumer

Subcommittee on Commerce, Trade, and Consumer Protection
July 14, 2004
11:30 AM

16. Barry Steinhardt (ACLU) statement con't

My name is Barry Steinhardt and I am the director of the Technology and Liberty Program at the American Civil Liberties Union (ACLU). The ACLU is a nationwide, non-partisan organization with nearly 400,000 members dedicated to protecting the individual liberties and freedoms guaranteed in the Constitution and laws of the United States. I appreciate the opportunity to testify about Radio Frequency Identification (RFID) tags on behalf of the ACLU before the Commerce, Trade and Consumer Protection Subcommittee of the House of Representatives Committee on Energy and Commerce. Today, I will explore with you the risks to privacy of governmental uses of RFID tags in identification documents, and the risks to consumer privacy of use of RFID tags by the private sector. I will close by suggesting that Congress play an active role in deciding whether to authorize governmental use of RFID tags in U.S. passports.

RFID tags are tiny computer chips connected to miniature antennae that can be placed on or in physical objects. The chips contain enough memory to hold unique identification codes for all manufactured items produced worldwide. When an RFID reader emits a radio signal, nearby tags respond by transmitting their stored data to the reader. With passive RFID tags, which do not contain batteries, read-range can vary from less than an inch to 20-30 feet, while active (self-powered) tags can have a much longer read range.

Drift toward a surveillance society

The privacy issues raised by RFID tags are vitally important because they are representative of a larger trend in the United States: the seemingly inexorable drift toward a surveillance society. As Congress considers the privacy issues posed by RFID chips, I urge you to view them in the larger context -- a world that is increasingly becoming a sea of data and databases, where the government and private corporations alike are gathering more and more details about our everyday existence.

The explosion of computers, cameras, sensors, wireless communication, GPS, biometrics, and other technologies in just the last 10 years is feeding what can be described as a surveillance monster that is growing silently in our midst. Scarcely a month goes by in which we don't read about some new high-tech method for invading privacy, from face recognition to implantable microchips, data-mining to DNA chips, and now RFID identity tags. The fact is, there are no longer any technical barriers to the creation of the surveillance society.

While the technological bars are falling away, we should be strengthening the laws and institutions that protect against abuse. Unfortunately, in all too many cases, even as this surveillance monster grows in power, we are weakening the legal chains that keep it from trampling our privacy. We should be responding to intrusive new technologies by building stronger restraints to protect our privacy; instead, all too often we are doing the opposite. (The ACLU has written a report on this subject, entitled *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, which is available on our Web site at www.aclu.org/privacy.)

17. Barry Steinhardt (ACLU) statement con't

We hope that this will not happen with RFID chips, which promise great new efficiencies and conveniences, but also hold the potential to enable the most Orwellian kinds of surveillance. RFID tags enable remote, even surreptitious identification; their use generally requires the creation of databases containing identity information; and RFID use is easily integrated into database systems and other technologies.

Congress must act to lay to rest the privacy fears surrounding this technology so that it will be smooth sailing for us all to enjoy its benefits.

There are two primary areas where RFIDs raise privacy issues: their use in retail and elsewhere in the commercial sector, and their direct adoption by government.

The most frightening use of RFID chips: government tracking

Government use of RFID is burgeoning. The Pentagon plans to use RFID to track physical objects – a use that raises relatively modest privacy concerns. Other proposed uses raise more serious concerns. The San Francisco Library, for example, is proposing to put RFID chips in its books, which raises the specter of third parties being able to track our reading habits without our knowledge.

Most troubling of all are proposals to incorporate RFID tags into government identity documents.

RFIDs would allow for convenient, at-a-distance verification of ID. RFID-tagged IDs could be secretly read right through a wallet, pocket, backpack, or purse by anyone with the appropriate reader device, including marketers, identity thieves, pickpockets, oppressive governments, and others. Retailers might add RFID readers to find out exactly who is browsing their aisles, gawking at their window displays from the sidewalk – or passing by without looking. Pocket ID readers could be used by government agents to sweep up the identities of everyone at a political meeting, protest march, or Islamic prayer service. A network of automated RFID listening posts on the sidewalks and roads could even reveal the location of all people in the U.S. at all times.

This may sound far-fetched, and I hope that it stays that way. But if we at the ACLU have learned anything over the past decade, it is that seemingly distant privacy invasions that sound right out of science fiction often become real far faster than anyone has anticipated. I give you this scenario as something that I think most Americans would agree is something that should be avoided, and yet is now entirely possible as far as the technology that is available to us. That means that our future is now going to be decided by policy.

RFID-powered documents: all-too real

We need not end up in the frightening situation that I have just described to suffer privacy invasions from RFID technology. In fact, worries about RFID-enabled identity documents are far from an abstract concern. Already, deliberations are underway to encourage governments to include RFID chips in the passport carried by citizens of every nation including the United States.

18. Barry Steinhardt (ACLU) statement con't

Largely unnoticed by the press and many public policy makers, an obscure UN-affiliated group called the International Civil Aviation Organization (ICAO) has been developing global standards for passports and other travel documents. This effort grows out of the Enhanced Border Security and Visa Entry Reform Act (EBSA), which mandated that the passport of every visa waiver country "issue to its nationals machine-readable passports that are tamper-resistant and incorporate biometric and document authentication identifiers;" any nation that fails to comply with this requirement will lose its status as a "visa-waiver" country. (1) The Act mandates that the standards for these passports be created by ICAO.

Under ICAO's current proposal, passports around the world would not only incorporate biometrics like fingerprints or face recognition, but -- as we only recently learned -- also remotely readable "contact-less integrated circuits," or RFID tags. Nothing in EBSA requires the inclusion of an RFID chip on passports.

While we'll be making this testimony available to other committees that would have a strong interest in whether RFID tags go on passports, we believe that a wholistic approach to the use of RFID tags by Congress may be called for.

ICAO has been developing these passport standards over a period of months in meetings held around the world. Because of the serious implications of creating an RFID-enabled identity document, the ACLU and the London-based group Privacy International tried to arrange attendance of a representative at a March 2004 meeting held in Cairo.

This effort was unsuccessful. An open letter to the ICAO on privacy concerns over the biometric standards likewise met with no response. (2) The ACLU again wrote to ICAO asking to attend a May 2004 meeting in Montreal, and once again received no response.

In short, despite the importance of technical and interoperability standards -- which can mean the difference between a use of biometrics that poses enormous problems for privacy, or one that poses little -- ICAO has ignored attempts by privacy and civil liberties groups to join in their process. To a degree that would not be possible with a domestic government decision-making body, it has rebuffed NGO attempts to provide input on the privacy implications of the particular standards being considered, or even simply to observe the meetings.

Like the results of most processes with limited input, the standards developed by the ICAO are deeply flawed. The RFID chips under consideration can be read from up to a meter away and have enough memory to hold full biometric information such as fingerprints or photographs. The potential uses and abuses of such a chip could be revolutionary. A retail store or restaurant, for example, might gain the ability to capture the identities of those who walk through a portal; a government official could instantly sweep the room to discover who is attending a political meeting. Imagine the uses to which a dictator like Fidel Castro could put such technology. Every person in Cuba -- including Cuban-Americans carrying U.S. passports while visiting family members in Cuba -- could be put under surveillance and no one would be safe.

19. Barry Steinhardt (ACLU) statement con't

If the United States mandates the creation of an international standard for passports, it will face enormous pressure to conform its own passports to that standard. For instance, when the US instituted the US Visit Program one nation, Brazil, reacted swiftly by putting similar measures into effect for just their American visitors. (3) In fact, far from being concerned that such systems would lead to the retaliatory creation of systems for tracking Americans elsewhere in the world, Bush Administration officials have embraced such reciprocation. "We welcome other countries moving to this kind of system," Department of Homeland Security undersecretary Asa Hutchinson declared. "We fully expect that other countries will adopt similar procedures." (4)

By instituting RFID chips in passports, the US government could skip right over the politically untenable proposals for a National ID card, and set a course toward the creation of a global identity document -- or, at least, toward a set of global standards for identity that can be incorporated into a wide variety of national identity documents. There are two possible paths by which RFID-powered passports could become tools for tracking the everyday lives of Americans:

-- These passports come to be seen as the gold standard of identity verification around the world. More and more, they are demanded as proof of identity not only abroad but within the United States as well, displacing driver's licenses as the primary form of identification in everyday life.

-- They become the template for standardized versions of the driver's license, turning them into a de facto National ID card.

Features such as the inclusion of a remotely readable RFID chip would greatly enhance the private sector's tendency to piggyback on the perceived "trust value" of these documents. Although theoretically optional, like driver's licenses and credit cards before them, they may quickly become what are for all practical purposes requirements for navigating through the modern world. The result would be a situation where the government gains a tremendous new power to track and control the movement of citizens.

Or innocent citizens, at any rate. We must always keep in mind that as the perceived "trust value" of such documents rises, and as their adoption becomes more widespread, the payoff for counterfeiting them also rises -- perhaps even more steeply -- with the result that counterfeit or fraudulently acquired real documents will continue to remain available to determined and well-financed wrongdoers. (5)

While we understand the desire of the ICAO to increase confidence in travel documents, reduce fraud, combat terrorism, and protect aviation security, the inclusion of RFID tags will have disproportionate and unnecessary effects on privacy and civil liberties. Developed without outside input, the ICAO passport has morphed from a simple identity document to become a de facto monitoring device. Worse, this monitoring device threatens to be foisted on the American public with little or no debate. Because of the power and potential of RFID chips, the actions of the ICAO threaten the rights of Americans and people around the world.

20. Barry Steinhardt (ACLU) statement con't

Consumer issues

The second major area where privacy concerns are raised by RFID tags in addition to government uses is the commercial side. Major retailers are engaged in a major push to advance adoption of RFID technology, and many envision RFIDs eventually replacing UPC bar codes on products.

Such a pervasive adoption of RFID technology raises profound privacy questions. The most detailed and often intimate picture of Americans' lives can be constructed through their consumer purchases. The issues were well explained in a position statement issued by a coalition of 30 consumer and privacy organizations. They include:

-- **Hidden placement of tags**. RFID tags can be embedded into/onto objects and documents without the knowledge of the individual who obtains those items. As radio waves travel easily and silently through fabric, plastic, and other materials, it is possible to read RFID tags sewn into clothing or affixed to objects contained in purses, shopping bags, suitcases, and more.

-- **Unique identifiers for all objects worldwide**. The Electronic Product Code potentially enables every object on earth to have its own unique ID. The use of unique ID numbers could lead to the creation of a global item registration system in which every physical object is identified and linked to its purchaser or owner at the point of sale or transfer.

-- **Massive data aggregation**. RFID deployment requires the creation of massive databases containing unique tag data. These records could be linked with personal identifying data, especially as computer memory and processing capacities expand.

-- **Hidden readers**. Tags can be read from a distance, not restricted to line of sight, by readers that can be incorporated invisibly into nearly any environment where human beings or items congregate. RFID readers have already been experimentally embedded into floor tiles, woven into carpeting and floor mats, hidden in doorways, and seamlessly incorporated into retail shelving and counters, making it virtually impossible for a consumer to know when or if he or she was being "scanned."

-- Individual tracking and profiling. If personal identity were linked with unique RFID tag numbers, individuals could be profiled and tracked without their knowledge or consent. For example, a tag embedded in a shoe could serve as a de facto identifier for the person wearing it. Even if item-level information remains generic, identifying items people wear or carry could associate them with, for example, particular events like political rallies.

Given the potential for widespread commercial use of RFID chips, we believe that Congress ought to step in and require privacy protections surrounding the use of this technology -- in particular, the incorporation into law of the fair information principles that are recognized around the world.

21. Barry Steinhardt (ACLU) statement con't

Government privacy and consumer privacy: not so separate

Although I have distinguished the privacy issues raised by the government's adoption of RFID tags and the private sector's, the difference between the two is quickly eroding from the perspective of individual privacy. Government security agencies are increasingly making an effort to make use of private sector information in anti-terrorism efforts that are oriented around vast sweeps through Americans' data in the hunt for terrorists. And the government's power to access private data is rapidly expanding through the Patriot Act and other measures.

In general, privacy concerns are more serious when they involve the government. But increasingly, the information that is collected about people by a retailer or other private-sector corporation can and is ending up in the hands of the government.

Conclusion

I believe that all the testimony you hear today will make clear that RFID chip technology is growing rapidly and has incredible potential for both use and abuse. I hope that my testimony has amplified two further points: this growth is taking place largely outside of the control of the US government and it will have significant impact on every American. What that impact will be has yet to be decided.

Congress must be vigilant and involved in how RFID technology is deployed. What is at stake is no less than how and when Americans will be identified and tracked here and around the world. We are at a pivotal juncture, where technology has presented us with the ability to implant monitoring devices on everything. And their use is being contemplated on perhaps the most fundamental travel document in the world. All without any guidance or direction from Congress or the American people.

The decisions Congress makes on RFID chips will affect the direction of this technology around the world. You must decide whether we want to go down the path of incorporating RFID into our identity documents or to choose a less invasive technology like the two-dimensional bar code. Over the longer term, the Congress needs to consider how the fair information principles that my fellow panelists have discussed can be applied to RFID and the many other new technologies that have placed us on the edge of becoming a surveillance society.

The debate must begin right now. If RFID technology is to be employed it must be carefully controlled, yet none of those controls currently exist. A fait accompli, presented by an unelected international body, is a real possibility. We urge you to be vigilant in monitoring these developments and creating legal controls to protect American privacy both domestically and internationally. Thank you.