RFID

Radio Frequency IDentification:

Applications and Implications for Consumers

A Workshop Report
from the Staff of the Federal Trade Commission

March 2005

Radio Frequency IDentification: Applications and Implications for Consumers

A Workshop Report from the
Staff of the Federal Trade Commission

March 2005

Federal Trade Commission

This is a report of the staff of the Federal Trade Commission. The views expressed in this report are those of the staff and do not necessarily represent the views of the Federal Trade Commission or any individual Commissioner. The Commission has voted to authorize the staff to publish this report.

Contents

I. Introduction

Radio frequency identification technology, known as RFID, has been described as "tech's official Next Big Thing."[1] RFID is not actually a new technology, but it is being applied in new ways, spurred by technological advances and decreased costs. Once used during World War II to identify friendly aircraft, RFID is now being used in a variety of public and private sector settings, from hospitals to the highway.

In RFID systems, an item is tagged with a tiny silicon chip and an antenna; the chip plus antenna (together called a "tag") can then be scanned by mobile or stationary readers, using radio waves (the "RF"). The chip can be encoded with a unique identifier, allowing tagged items to be individually identified by a reader (the "ID"). Thus, for example, in a clothing store, each particular suit jacket, including its style, color, and size, can be identified electronically. In a pharmacy, a druggist can fill a prescription from a bottle bearing an RFID-chipped label confirming the authenticity of its contents. On the highway, cars with RFID tags on their windshields can move swiftly through highway tollbooths, saving time and reducing traffic congestion. At home, pets can be implanted with chips so that lost animals can be identified and returned to their owners more readily. In each case, a reader must scan the tag for the data it contains and then send that information to a database, which interprets the data stored on the tag. The tag, reader, and database are the key components of an RFID system.

RFID proponents believe that the ability of these systems to deliver precise and accurate data about tagged items will improve efficiency and bring other benefits to businesses and consumers alike.[2] One major retailer has already announced a mandate for its largest suppliers to begin tagging cases and pallets of merchandise.[3] Other companies in the U.S. and abroad reportedly are exploring similar directives.[4] Spending on RFID implementation in the retail supply chain alone has been estimated at $91.5 million last year – an amount expected by some to exceed $1 billion by 2007.[5] Outside the retail sector, libraries across the country reportedly are already tagging books,[6] and the FDA has announced that it is actively encouraging pharmaceutical manufacturers to use RFID to fight drug counterfeiting.[7]

While these developments may offer significant benefits for industry and consumers, some applications have raised privacy concerns. The capacity to encode unique identifiers at the individual item level may have revolutionized thinking about inventory management, but it has also raised fears that this technology might be used to track individual products out of the store and into consumers' homes or otherwise monitor individual consumer behaviors. As with the Internet and other data-intensive technologies, these concerns must be addressed so that they do not hinder the development and deployment of RFID in the marketplace.

On June 21, 2004, the Federal Trade Commission explored these issues at a public workshop entitled "Radio Frequency Identification: Applications and Implications for Consumers." The Workshop brought together technologists, RFID proponents, privacy advocates, and policymakers to discuss the range of applications for RFID, the future of this technology, and its implications for consumers.[8] This staff report will summarize the discussion at the Workshop and offer some preliminary recommendations for addressing the privacy concerns raised by some participants.[9]

Part I of the report provides an overview of the issues the report covers and a summary of the FTC staff's conclusions. Parts II through V summarize the Workshop panel discussions and highlight some of the key points made in the written comments submitted to the Commission in connection with the Workshop. Specifically, Part II discusses how RFID technology works. Part III describes current and emerging uses of RFID technology, both in the private and public sectors. Part IV discusses the consumer privacy implications of RFID applications and database security issues. Part V describes different proposals to address consumer privacy concerns, including technological approaches and self-regulatory efforts. Finally, Part VI offers Commission staff conclusions regarding steps that RFID users may take to alleviate RFID-related privacy concerns.

As explained in Part VI below, based on the information received in connection with the Workshop and other available information, the FTC staff concludes:

- Industry initiatives can play an important role in addressing privacy concerns raised by certain RFID applications. The goal of such programs should be transparency.

- Any industry self-regulatory program should include meaningful accountability provisions to help ensure compliance.

- Many of the potential privacy issues associated with RFID are inextricably linked to database security. As in other contexts in which personal information is collected from consumers, a company that uses RFID to collect such information must implement reasonable and appropriate measures to protect that data.

- Consumer education is a vital part of protecting consumer privacy. Industry members, privacy advocates, and government should develop education tools that inform consumers about RFID technology, how they can expect to encounter it, and what choices they have with respect to its usage in particular situations.

II. The ABCs of RFID

Understanding what RFID devices are and how they work is critical to an analysis of the policy issues surrounding this technology. Generic references to "RFID technology" may be applied incorrectly to a wide range of devices or capabilities. For example, RFID by itself is not a location-tracking technology. At sites where readers are installed, RFID may be used to track tagged objects, but this static readability differs from technology such as global positioning systems, or GPS, which uses a network of satellites to pinpoint the location of a receiver.[10] And RFID technology itself can be used for a variety of applications, from contactless identification cards that can be scanned no farther than inches away from a reader, to highway systems utilizing "active" RFID tags that can initiate communication with a scanner 100 feet away.

A. Primary Components of RFID Devices

RFID devices have three primary elements: a chip, an antenna, and a reader. A fourth important part of any RFID system is the database where information about tagged objects is stored.

- **The chip**, usually made of silicon, contains information about the item to which it is attached. Chips used by retailers and manufacturers to identify consumer goods may contain an Electronic Product Code ("EPC").[11] The EPC is the RFID equivalent of the familiar universal product code ("UPC"), or bar code, currently imprinted on many products. Bar codes must be optically scanned, and contain only generic product information. By contrast, EPC chips are encrypted with a *unique* product code that identifies the individual product to which it is attached, and can be read using radio frequency. These codes contain the type of data that product manufacturers and retailers will use to track the authenticity and location of goods throughout the supply chain.

  An RFID chip may also contain information other than an EPC, such as biometric data (a digitized image of a fingerprint or photograph, for example).[12] In addition, some chips may not be loaded with information uniquely identifying the tagged object at all; so-called "electronic article surveillance systems" ("EAS") may utilize radio frequency communication to combat shoplifting, but not to uniquely identify individual items.

- **The antenna** attached to the chip is responsible for transmitting information from the chip to the reader, using radio waves. Generally, the bigger the antenna, the longer the read range. The chip and antenna combination is referred to as a transponder or, more commonly, as a tag. Participants at the workshop brought samples of tags currently in use. The pictures below show a common EPC tag that can be affixed to an object (Figure A) and a paper hang-tag that can be attached to individual articles of clothing (Figure B[13]).

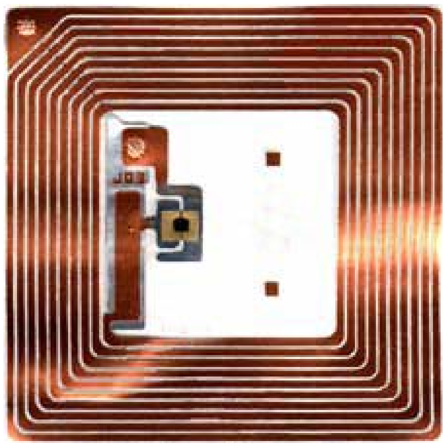


Figure A. EPC tag

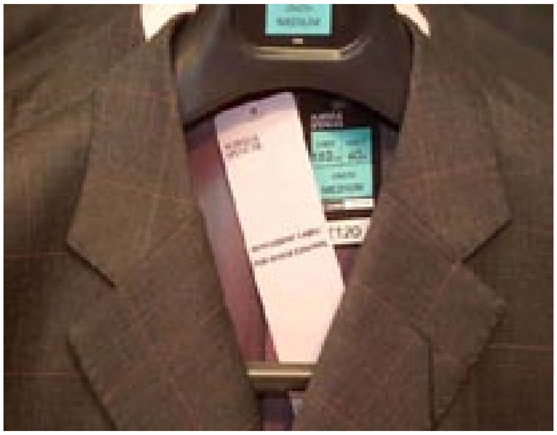


Figure B. RFID hang-tag

- **The reader**, or scanning device, also has its own antenna, which it uses to communicate with the tag.[14] Readers vary in size, weight, and power, and may be mobile or stationary. Although anyone with access to the proper reader can scan an RFID tag,[15] RFID systems can employ authentication and encryption to prevent unauthorized reading of data.[16] "Reading" tags refers to the communication between the tag and reader via radio waves operating at a certain frequency. In contrast to bar codes, one of RFID's principal distinctions is tags and readers can communicate with each other without being in each other's line-of-sight.[17] Therefore, a reader can scan a tag without physically "seeing" it. Further, RFID readers can process multiple items at one time, resulting in a much-increased (again as compared to UPC codes) "speed of read."[18]

  The pictures on the opposite page show various RFID readers: a stationary reader that could be used to track tagged cases of goods entering a warehouse (Figure C[19]); a mobile reader used to monitor inventory on a retail store floor (Figure D[20]); and a prototype of a glove embedded with a scanner used to track daily domestic living activities (Figure E[21]).

- **The database**, or other back-end logistics system, stores information about RFID-tagged objects. Access to both a reader and its corresponding database are necessary before information stored on an RFID tag can be obtained and understood. In order

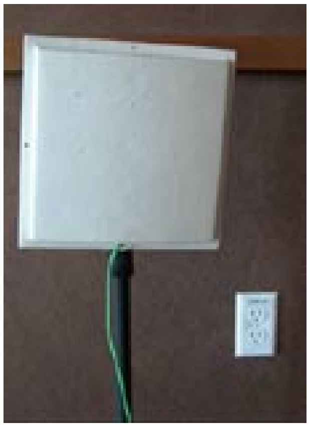


Figure C. Stationary reader

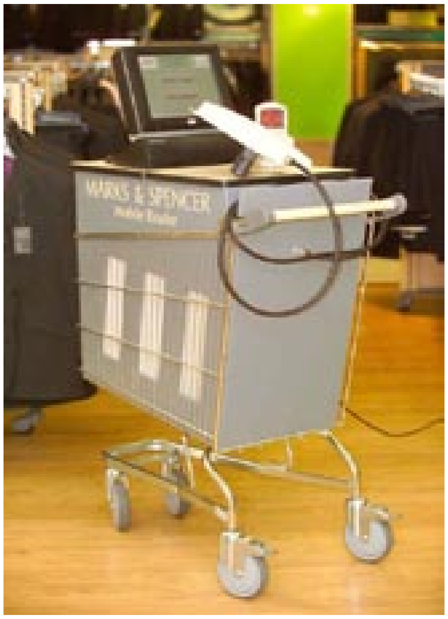


Figure D. Mobile reader

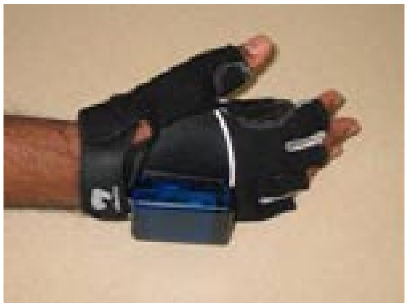


Figure E. Reader-embedded glove

to interpret such data, RFID readers must be able to communicate with a database or other computer program.

One protocol being developed for product manufacturers uses chips embedded with a 96-bit EPC code – a number – that includes several fields identifying the manufacturer (“ABC Company”), the product (“cola”), its size or its packaging (“24-pack of cola cans”), and a unique identifier.[22] This system, the “EPCglobal Network,” calls for a secure network of servers that will share information obtained from tagged objects moving through the supply chain. According to the network’s architect, EPCglobal, the data will be stored on EPCglobal member company databases, access to which will be controlled by those individual companies.[23] In order to interpret what these fields mean, a directory, or “object naming service” (“ONS”), will direct the reader to the appropriate server(s) where the data from the tag and associated information are stored. The ONS will function much like a reverse telephone directory or an Internet browser, which translates a URL into a Web site.[24] In the RFID context, the ONS will identify what server has information about the tagged item, allowing an RFID user to interpret the meaning of the particular code on a particular tag.[25] The database information will vary with the context. For example, with automatic highway toll payment systems, databases will link account numbers stored on a tag to the appropriate prepaid account for billing purposes.[26]

Although all RFID systems have these essential components, other variables affect the use or set of applications for which a particular tag is appropriate. As discussed further below, key factors include whether the tag used is “active” or “passive”; what radio frequency is used; the size of the antennas attached to the chip and to the reader; what and how much information can be stored on a tag; and whether the tag is "read/write" or "read-only." These factors affect the read ranges of the systems as well as the kind of object that can usefully be tagged. They also impact the cost, which is an especially important commercial consideration when tagging a large volume of items.

B. Passive v. Active Tags

There are three types of RFID tags, differentiated by how they communicate and how that communication is initiated:

- **Passive tags** have no onboard power source – meaning no battery – and do not initiate communication. A reader must first query a passive tag, sending electromagnetic waves that form a magnetic field when they "couple" with the antenna on the RFID tag."[27] Consistent with any applicable authorization, authentication, and encryption, the tag will then respond to the reader, sending via radio waves the data stored on it. Currently, depending on the size of the antenna and the frequency, passive tags can be read, at least theoretically, from up to thirty feet away. However, real-world environmental factors, such as wind and interference from substances like water or metal, can reduce the actual read range for passive tags to ten feet or less.[28] Passive tags are already used for a wide array of applications, including building-access cards, mass transit tickets, and, increasingly, tracking consumer products through the supply chain. Depending on the sophistication of the chip, such as how much memory it has or its encryption capability, a passive tag currently costs between 20 cents and several dollars.[29]

- **Semi-passive tags**, like passive tags, do not initiate communication with readers, but they do have batteries. This onboard power is used to operate the circuitry on the chip, storing information such as ambient temperature. Semi-passive tags can be combined, for example, with sensors to create "smart dust" – tiny wireless sensors that can monitor environmental factors. A grocery chain might use smart dust to track energy use, or a vineyard to measure incremental weather changes that could critically affect grapes.[30] Devices using smart dust, also known as "motes," currently cost about $100 each, but, in a few years, reportedly could drop to less than $10 apiece.[31]

- **Active tags** can initiate communication and typically have onboard power. They can communicate the longest distances – 100 or more feet. Currently, active tags typically cost $20 or more.[32] A familiar application of active tags is for automatic toll payment systems, like the Northeast's "E-ZPass," that allow cars bearing active tags to use express lanes that don't require drivers to stop and pay.[33]

C. Radio Frequency

Communication between RFID tags and readers is also affected by the radio frequency used, which determines the speed of communications as well as the distance from which tags can be read. Higher frequency typically means longer read range. Low-frequency ("LF") tags, which operate at less than 135 kilohertz (KHz), are thus appropriate for short-range uses, like animal identification and anti-theft systems, such as RFID-embedded automobile keys.[34] Systems that operate at 13.56 megahertz (MHz) are characterized as high frequency ("HF"). Both low-frequency and high-frequency tags can be passive. Scanners can read multiple HF tags at once and at a faster rate than LF tags. A key use of HF tags is in contactless "smart cards," such as mass transit cards or building-access badges.[35]

The third frequency, Ultra-High Frequency ("UHF"), is contemplated for widespread use by some major retailers, who are working with their suppliers to apply UHF tags to cases and pallets of goods. These tags, which operate at around 900 MHz, can be read at longer distances, which outside the laboratory environment range between three and possibly fifteen feet.[36] However, UHF tags are more sensitive to environmental factors like water, which absorb the tag's energy and thus block its ability to communicate with a reader.

D. Read/Write Capacity

Finally, another important feature of RFID tags is their "read/write" capacity, or "read-only" status. These terms refer to a tag's ability to have data added to it during its lifetime. The information stored on a "read-only" tag cannot be altered, but a writeable tag (with read/write capacity) can receive and store additional information. Read/write applications are most prevalent when tags are re-used.[37] They are usually more sophisticated and costly than read-only applications. In addition, read/write applications have shorter read ranges. Read-only tags are well-suited to applications like item-level tagging of retail goods, since they are less expensive and, as part of a networked system, can provide a great deal of information by directing the reader to the associated database(s) where information about the tagged item is maintained.[38]

III. RFID Today and Tomorrow

The Workshop included a comprehensive discussion of RFID's various current and anticipated applications. Both private and public sector users of RFID explained how they are applying this technology to improve their delivery of goods and services. Privacy advocates also addressed the implications of these initiatives, sounding a cautionary note about some of the emerging uses of RFID and their consequences for consumer privacy.

A. Current Uses of RFID

Workshop participants described a number of RFID applications that consumers may already be using. For example, some consumers are familiar with employee identification cards that authenticate the pass-holder before permitting access.[39] A related use of RFID is for event access – to amusement parks, ski areas, and concerts, where tagged bracelets or tickets are used.[40] Panelists also explained how RFID is being used in a variety of transportation-related contexts. Many automobile models already use RFID tags in keys to authenticate the user, adding another layer of security to starting a car.[41] Another example, the "Speedpass," allows drivers to purchase gas and convenience store goods from ExxonMobil stations.[42] RFID is also transforming highway travel, with the advent of E-ZPass in Northeastern and Mid-Atlantic states and similar programs in other regions of the country that allow drivers to pass through tolls without stopping to pay. An active tag on the vehicle's windshield lets a reader installed at the tollbooth know that a tagged vehicle is passing through; information flows from the tag, to the reader, and then to a centralized database, where the prepaid or checking account associated with that vehicle is charged.[43]

B. RFID in the Supply Chain

To the extent that the much-touted "RFID revolution" is underway, it is occurring somewhat out of public sight – in warehouses, distribution centers, and other stages of the supply chain.[44] Workshop participants discussed how RFID's impact on the flow of goods through distribution channels has implications not just for manufacturers, suppliers, and retailers, but also for consumers.[45] Many panelists reported that as a result of more efficient distribution practices generated by RFID use, consumers may find what they want on the store shelves, when they want it, and perhaps at lower prices.[46]

Workshop participants representing manufacturers and retailers described the anticipated economic benefits of RFID. According to one panelist, the retail industry suffers losses between $180 and $300 billion annually because of poor supply chain visibility – the inability to track the location of products as they make their way from manufacturer to retailer.[47] As a result, this panelist stated, retailers are not always able to keep high-demand goods in stock, or they may have inventory that they can't move.[48]

Participants discussed how RFID may help prevent these lapses by improving visibility at multiple stages of the supply chain. RFID readers can gather information about the location of tagged goods as they make their way from the manufacturer, to a warehouse or series of distribution centers, and to the final destination, their store.[49] Also, as one workshop participant explained, RFID enhances the accuracy of information currently obtained through bar code scanning, which is more vulnerable to human error.[50] According to this panelist, access to more – and more accurate – information about where products are in the distribution chain enables retailers to keep what they need in stock and what they do not need off the shelf.[51]

Workshop participants also touted the discipline that RFID imposes on the supply chain by, for example, reducing "shrinkage," or theft.[52] One panelist explained how RFID may lower costs by keeping shipping volumes leaner and more accurate.[53] Other panelists described how RFID tags can be read much faster than bar codes, citing tests indicating that RFID's scanning capability can result in goods moving through the supply chain ten times faster than they do when bar codes are used.[54] According to another participant, RFID will facilitate quicker, more accurate recalls by enabling the tracking of a product's origin and its location in the distribution chain.[55] Further, this panelist asserted, RFID will enhance product freshness by monitoring expiration dates of consumer goods, so retailers know when not to offer items for sale.[56]

C. RFID Use in the Public Sector

Panelists also discussed how RFID is being used or contemplated for use by government entities to meet objectives similar to those their private-sector counterparts hope to achieve. Workshop participants discussed a variety of ongoing and proposed government RFID applications, from the U.S. Department of Defense's ("DoD") October 2003 mandate requiring its suppliers to use RFID tags by January 2005 to local library systems deploying this technology to track and trace their books.[57] DoD's initiative reportedly will affect 43,000 military suppliers.[58] And, according to panelists, public libraries in California, Washington State, and elsewhere have implemented internal RFID systems to facilitate patron usage and manage stock.[59]

One Workshop panelist, representing the U.S. Food and Drug Administration ("FDA"), highlighted that agency's RFID initiative.[60] Although the FDA itself is not using this technology, it recently announced an initiative to promote the use of RFID in the pharmaceutical supply chain by 2007.[61] For now, drug manufacturers will primarily tag "stock bottles" – those used by pharmacists to fill individual prescriptions – but eventually consumers may be purchasing packages labeled with RFID chips.[62] The core objective of this initiative is to fight drug counterfeiting by establishing a reliable pedigree for each pharmaceutical.[63] The FDA believes that this goal can most effectively be accomplished by its target date through the adoption of RFID, which offers distinct advantages over other identification systems that require line-of-sight scanning and are not as accurate or fast.[64]

Another government entity turning to RFID is the U.S. Department of Homeland Security ("DHS"). One program described by a DHS official at the Workshop uses RFID for tracking and tracing travelers' baggage.[65] Both individual airports[66] and airlines[67] will use RFID technology to identify and track passenger luggage, from check-in to destination. Another DHS initiative addressed at the Workshop involves the agency's "US-VISIT" (U.S. Visitor and Immigrant Status Indicator Technology) program. That initiative will test RFID at the country's fifty busiest border-crossing locations by using RFID to read biometric identifiers, such as digital photographs and fingerprint scans, embedded in U.S. work visas issued to foreign nationals.[68] According to the DHS representative, this program is expected to facilitate some of the approximately 330 million border-crossings each year by getting "the appropriate level of information to the right people at the right time."[69] As this panelist noted as well, U.S. passports will also soon carry an RFID chip embedded with identifying information, including biometric data.[70]

D. Emerging RFID Applications

The Workshop also addressed emerging RFID applications and when such uses are expected to be implemented. According to panelists, one sector that is the focus of extensive RFID research is health care, where RFID devices can be used to track equipment and people within a medical facility.[71] Other proposed applications contemplate using RFID in different ways. For example, one ongoing study discussed at the Workshop is exploring how RFID can enhance the quality of elder care.[72] By tagging key objects in a senior's home – such as prescription drug bottles, food items, and appliances – and embedding small RFID readers in gloves that can be worn by that individual, that person's daily habits can be monitored remotely by a caregiver.[73] This system would develop more accurate record-keeping for medical treatment purposes and could facilitate independent living for senior citizens.[74]

The Workshop also addressed the anticipated timeline for the adoption of item-level RFID tagging in the retail sector. According to one participant, some retailers are currently experimenting with embedding RFID tags in individual consumer goods, and cited as an example German retailer Metro AG's controversial use of RFID in its "Future Store."[75] However, many panelists concurred that widespread item-level tagging of retail products was not imminent.[76] The most commonly cited reason for this delay was cost: according to one panelist, the current price per tag of between 20 and 40 cents makes item-level RFID too expensive to deploy widely in the near term.[77] Workshop panelists also asserted that the target cost of five cents per tag will likely not be realized until 2008.[78] Even then, other costs may slow the evolution of item-level tagging. According to one Workshop participant, hardware costs account for only 3% of the expense of deploying RFID. Expenditures for developing the software necessary to interpret and store information generated by RFID constitute nearly three-quarters of the cost of implementing this technology.[79]

According to Workshop participants, other factors that could inhibit the evolution of item-level tagging include the lack of standardization for RFID frequency and power; inadequate end-user knowledge about how the technology works; and technical challenges, such as reader accuracy and interference from external substances (like water and metal).[80]

IV. Consumer Perceptions and Privacy Concerns

A. Consumer Survey Results

In addition to addressing how RFID works and can be used, Workshop participants discussed the implications of this technology for consumers. The Workshop included a presentation about the results of a study concerning consumer perceptions of RFID. According to a survey of more than 1,000 U.S. consumers conducted in October 2003, the majority of those polled were unfamiliar with RFID.[81] Over three-quarters of the sample – 77% – had not heard of RFID. Confirming the general lack of knowledge about this technology, nearly half of the group aware of RFID had "no opinion" about it.[82]

Consumers who did have an opinion about RFID expressed a variety of views about whether or how this technology would affect them. When asked to rank a set of potential benefits of RFID, 70% identified recovery of stolen goods and improved food and drug safety high on the list. The majority (66%) also placed cost savings toward the top of the list of benefits, although some consumers were also concerned that RFID use would instead raise prices. Consumers placed access to marketing-related benefits, like in-aisle companion product suggestions, at the bottom of the list.[83]

The most significant concerns expressed by consumers familiar with RFID related to privacy. In response to both open-ended and prompted questions (with pre-programmed answers to select or rank), privacy emerged as a leading concern. For example, approximately two-thirds of consumers identified as top concerns the likelihood that RFID would lead to their data being shared with third parties, more targeted marketing, or the tracking of consumers via their product purchases. These findings are consistent with the views of consumers who submitted comments to the Commission about RFID.[84] Many of those consumers voiced strong opposition to having RFID devices track their purchases and movements, with some citing as reasons for their position the potential for increased marketing or government surveillance.

A more recent consumer survey, conducted by two market research companies, revealed similar results.[85] Of more than 8,000 individuals surveyed, fewer than 30% of consumers were aware of RFID technology. Further, nearly two-thirds of all consumers surveyed expressed concerns about potential privacy abuses.[86] Their primary concerns centered around

RFID's ability to facilitate the tracking of consumers' shopping habits and the sharing of that information among businesses and with the government. Like the study discussed at the Workshop, this survey also demonstrated that the great majority of consumers remain unfamiliar with RFID. Additionally, consumers who fell into the "RFID non-aware" category were more likely to be concerned about RFID's implications for their privacy than were consumers who were familiar with the technology.[87]

B. RFID and Consumer Privacy

Against the backdrop of survey data about consumer perceptions of RFID, Workshop participants discussed the nature of privacy concerns associated with some of the emerging uses of this technology. While there was some consensus among Workshop panelists that certain uses of RFID today – such as in the supply chain – may not jeopardize consumer privacy,[88] a number of consumer advocates voiced concerns about the potential impact of other RFID applications on consumer privacy.[89] According to these panelists, such concerns may arise when consumers interact more directly with tags and readers, particularly in the context of item-level tagging of retail goods.

The concerns articulated by these Workshop participants implicated issues specific to RFID technology as well as more general privacy issues. Some panelists discussed how RFID's unique or distinguishing characteristics may jeopardize consumer privacy. First, these participants cited as a key concern the "bit capacity" of Electronic Product Codes ("EPCs"), which enable the assignment of individual identifiers to tagged objects.[90] They argued that RFID's potential to identify items uniquely facilitates the collection of more – and more accurate – data.[91]

Other features of RFID that troubled these Workshop participants related to the devices' physical attributes. According to these panelists, the small size of tags and readers enables them to be hidden from consumers.[92] One Workshop participant explained that if a long read-range is not required, scanners can be smaller than a U.S. quarter.[93] Another Workshop participant focused on the privacy implications of the small size of RFID chips and how their shrinking dimensions facilitate their unobtrusive integration into consumer goods.[94] Some panelists highlighted the ability of RFID devices to communicate with one another through materials, without line-of-sight, and at some distance.[95] These technical characteristics, they argued, distinguish RFID from bar codes, which in order to be read must be visible on the outside of product packaging.[96] Some commenters pointed to these characteristics as evidence that RFID would allow surreptitious scanning to gather information about the products consumers wear or carry.[97] Participants also raised concerns about what they termed the "promiscuity" of RFID devices[98] – when tags can be accessed by multiple readers, it raises the specter of unfettered third-party surveillance.[99]

The combination of these factors, some Workshop participants asserted, will weaken consumers' ability to protect themselves from in-store tracking and surreptitious monitoring in public places, at work, and even at home. Certain panelists were especially concerned about RFID's potential to facilitate consumer tracking, by linking personally identifiable information in databases to the unique numbers on RFID tags. One participant described how a retailer could associate purchaser data with the uniquely identified product an individual buys.[100] According to the participant, this practice would be similar to what retailers can currently do with customer loyalty cards or credit cards.[101] However, a number of Workshop panelists maintained that RFID poses greater threats to consumer privacy because of the enhanced level of information it provides about *each* tagged item. They suggested that a tagged item carried by a consumer out of a store could be read covertly, and what it communicates could be more than just the presence of a particular item. If linked to purchase data, the identification of a particular product could also identify the individual who bought that item.[102]

Privacy advocates at the Workshop cited this latter potential as the basis for another privacy concern: consumer profiling. By tracking the movement of tagged goods and the people associated with them, more information can be gathered about the activities of those individuals.[103] That in turn could make it easier to predict the behavior of others who buy the same items, even without monitoring them.[104] Another concern raised at the Workshop relates to RFID's facilitation of "customer relationship management," whereby retailers customize pricing and service based on a consumer's potential profitability.[105] According to one Workshop participant, if RFID tags were embedded in customer loyalty cards, consumers could be identified as soon as they entered the store that issued the card. This could result in targeted marketing or customer service directed at the consumer, depending on his or her purchase history or other information linked to the loyalty card.[106]

Many of these fears are associated with item-level tagging. As noted in Section III.D., however, a number of Workshop participants representing retailers and other RFID users maintained that RFID was not being used in this manner on a widespread basis now and would not be in the near future.[107] Some panelists also argued that no real business case exists for the adoption of a network accessible to multiple users that contains information about these users' RFID-tagged goods. As one participant stated, "Wal-Mart doesn't want its competitors to read tags that are from Wal-Mart stores. Wal-Mart probably also doesn't want its suppliers to read information about its other suppliers. They want to control that information for competitive reasons."[108]

Even if and when item-level tagging is adopted on a widespread basis, some Workshop participants disputed that consumer privacy would be jeopardized as a result. They asserted that RFID's technological limitations will prevent its surreptitious use. For example, reading an RFID tag from a significant distance currently requires use of a sizable antenna ("about the size of a plate," according to one panelist) and significant energy.[109] Another argument advanced at the Workshop focused on how cost factors will continue to slow retailers' adoption of RFID, limiting the sophistication and proliferation of readers on the store floor.[110] One participant representing a retail chain argued that no business case exists for linking data collected via RFID to personally identifiable information about consumers, so fears about this potential are misplaced.[111] In addition, many panelists addressed the emergence of a variety of technological protocols and products, such as encryption and blocker tags, that may offer a means to address privacy concerns associated with these devices.[112]

C. Database Security Issues

Regardless of panelists' views regarding the existence or extent of many privacy concerns, many participants agreed that database security was an important issue, especially in the manufacturing and retail environment. Rather than concentrating on how information may be collected via RFID devices, these participants discussed security issues that focus on how such data is stored and whether it is adequately protected.[113] According to one panelist, database security is a critical aspect of any analysis of privacy concerns associated with RFID use, because the tags themselves may contain only limited data, such as a number in the case of EPC chips.[114] The panelist further explained that the information associated with that number will be stored on a server of the product manufacturer or other authorized user, where it can be linked to additional data.[115]

Although Workshop panelists did not analyze the specific database security concerns linked to RFID use, one commenter provided a detailed discussion of these issues.[116] According to this commenter, security concerns are likely to arise in connection with interoperable tags, which can be read by different enterprises sharing information associated with those tags.[117] The commenter explained that the security of any database in which that information is stored depends on traditional information technology protections – not RFID-specific practices.[118] Further, the commenter asserted that these concerns are exacerbated when databases are maintained by third parties, outside of the RFID user's direct control.[119] Thus, the commenter argued, security measures will be that much more critical if databases contain information from RFID tags linked to personally identifiable information about the purchasers of tagged items.[120]

Workshop participants representing a range of interests generally acknowledged the need to address these issues. One speaker emphasized that the EPCglobal Network will maintain the security of data associated with EPC tags, which will be stored on servers "beyond the firewalls of corporations, logistics providers and retailers all around the globe."[121] However, others felt that insufficient attention has been devoted to database security[122] and maintained that RFID use will exacerbate existing concerns, since information collected via RFID will be that much more detailed and accurate.[123] Another Workshop participant argued that the focus on privacy concerns presented by RFID devices (i.e., tags and readers) are obfuscating the more important concerns related to general database security.[124]

V. Addressing Consumer Privacy Challenges: Best Practices and Principles

The Workshop concluded with a panel examining various approaches to addressing the privacy issues raised by RFID technology. As participants noted, these challenges are not insubstantial, in light of RFID's evolving nature and the uncertainty as to how various existing and potential uses may affect consumers.[125] Industry guidelines, legislative developments, and technological solutions designed to address privacy and security concerns were among the options discussed and debated.[126]

A. Existing Industry Practices and Standards

Panelists voiced a range of opinions as to what approach or combination of measures would be most effective at meeting the challenges posed by RFID. Many participants agreed that, at a minimum, businesses deploying RFID should take steps to protect consumer privacy. One self-regulatory model already in place is EPCglobal's "Guidelines on EPC for Consumer Products" ("EPCglobal Guidelines").[127] According to a Workshop panelist, the Guidelines were developed with input from privacy experts and apply to all EPCglobal members.[128] The Guidelines call for consumer notice, choice, and education, and also instruct companies to implement certain security practices.[129]

The first element, consumer notice, requires that companies using EPC tags "on products or their packaging" include an EPC label or identifier indicating the tags' presence. According to a Workshop participant, EPCglobal has developed a template label that companies can use to inform consumers of the presence of EPC tags.[130] Displaying a copy of the model identifier, the speaker explained that the template label discloses that a particular product's packaging contains an EPC tag, which may be discarded by a consumer after purchase.[131]

The Guidelines' second requirement, consumer choice, concerns the right of consumers to "discard or remove or in the future disable EPC tags from the products they acquire." The Guidelines explain, "for most products, the EPC tags [would] be part of disposable packaging or would be otherwise discardable."

Consumer education is the third prong of the Guidelines, which provides that consumers should have "the opportunity easily to obtain accurate information about EPC tags and their applications." The Guidelines task companies using RFID with "familiariz[ing] consumers with the EPC logo and . . . help[ing] consumers understand the technology and its benefits."

Finally, the Guidelines call for companies to ensure that any "data which is associated with EPC is collected, used, maintained, stored and protected" consistent with "any applicable laws."[132] They further instruct companies to publish "information on their policies regarding the retention, use and protection of any personally identifiable information associated with EPC use."[133] To help ensure compliance with these Guidelines, EPCglobal will provide a forum to redress complaints about failures to comply with the Guidelines.[134]

According to Workshop participants, some companies have already endorsed or implemented these practices as they test RFID systems.[135] Panelists discussed how Wal-Mart, which is currently operating a pilot program with EPC tags in a limited number of stores, has posted a "shelf-talker" disclosing the presence of EPC tags.[136] According to this tear-off notice reportedly made available to Wal-Mart shoppers, only cases of certain products or specific large items, like computer printers, include EPC tags and bear the EPCglobal logo. The disclosure further explains that the technology "will not be used to collect additional data about [Wal-Mart's] customers or their purchases."[137] Consistent with that commitment, Wal-Mart has stated that it has no readers on store floors, so consumers should not be exposed to any communications between tags and readers.[138]

Workshop panelists also discussed the privacy guidelines adopted by Procter & Gamble ("P&G"), another company involved in RFID trials both in the U.S. and abroad.[139] In addition to its global privacy policy, P&G has developed an RFID-specific position statement calling for "clear and accurate" notice to consumers about the use of RFID tags and consumer choice with respect to disabling or discarding EPC tags "without cost or penalty" as well as disclosure of whether any personally identifiable information about them is "electronically linked to the EPC number on products they buy."[140] Further, P&G stated at the Workshop that it will not participate in item-level tagging with any retailer or partner that would link personal information about consumers using RFID, "other than what they do for bar codes today."[141]

The Workshop also explored a case study of retail item-level RFID tagging in action. A representative of Marks & Spencer, one of the United Kingdom's largest retailers, described his company's in-store RFID pilot program, tagging menswear in select stores. Marks & Spencer's use of "Intelligent Labels," as it has designated its RFID program, is for stock control – a continuation of the supply chain management process.[142] With this limited purpose in mind, the Marks & Spencer official explained how his company incorporated privacy-protective measures into its Intelligent Label program.[143] According to the company, these considerations are reflected in the mechanics of its RFID deployment, which apply the notice, choice, and education principles advocated by EPCglobal and others. The hang-tags bearing the Intelligent Labels are large, visibly placed, and easily removable.[144] No data is written to the tags, and they are not scanned at the cash register, so there is no possibility of connecting the unique identifier on the tag to the purchaser. Indeed, the tags are not scanned at all during store hours, but rather are read for inventory control purposes when customers are not present. Finally, all of these practices are described in a leaflet that Marks & Spencer makes available to shoppers.[145]

Some Workshop participants stated that these industry initiatives represent effective ways to address consumer privacy concerns, but others maintained they are necessary, but insufficient, steps. Privacy advocates at the Workshop called for merchants to take additional precautions when using RFID tags on consumer items, including fully transparent use of RFID.[146] With respect to company statements disclosing the presence of in-store RFID devices, privacy advocates argued that such disclosures should be clear and conspicuous.[147] One participant stated that disclosures should contain specific information: that a product bears an RFID tag; that the tag can communicate, both pre- and post-purchase, the unique identification of the object to which it is attached; and the "basic technical characteristics of the RFID technology."[148] Another Workshop panelist urged that any such disclosures be "simple and factual," avoiding "happy face technology" that is essentially "marketing hype."[149] This panelist felt that by disclosing its RFID practices in a straightforward manner, a company will convey information in a way that consumers are more likely both to understand and trust.[150]

B. Regulatory Approaches

Privacy advocates at the Workshop also called for RFID to be subjected to a "formal technology assessment," conducted by a neutral body and involving all relevant stakeholders, including consumers.[151] This process could examine issues such as whether RFID can be deployed in less privacy-intrusive ways.[152] Until such an assessment takes place, these participants requested that RFID users voluntarily refrain from the item-level tagging of consumer goods.[153]

In addition, some Workshop panelists argued that government action to regulate RFID is necessary.[154] One panelist urged the Commission to implement a set of guidelines for manufacturers and retailers using RFID on consumer products.[155] According to this participant, other international standards that already apply to the use of RFID in this context support the need for comparable regulation in the U.S.[156] Certain Workshop participants also endorsed specific restrictions on RFID use, including prohibitions on tracking consumers without their "informed and written consent" and on any application that would "eliminate or reduce [individuals'] anonymity."[157] In addition, these participants called for "security and integrity" in using RFID, including the use of third-party auditors that could publicly verify the security of a given system.[158] Similarly, one panelist argued that consumers should be able to file with designated government and industry officials complaints regarding RFID users' non-compliance with stated privacy and security practices.[159]

Other Workshop panelists disputed the need for regulation at this point, contending that legislation could unreasonably limit the benefits of RFID[160] and would be ill-suited to regulate such a rapidly evolving technology.[161] According to one participant, the FTC's existing enforcement authority is adequate to address abuses of RFID technology, citing the Commission's ability to challenge misrepresentations by a company about its privacy and/or security practices.[162] Therefore, this participant concluded that technology-specific privacy legislation is unnecessary at this juncture.[163]

C. Technological Approaches

Workshop participants also debated the merits of various technological approaches to addressing consumer privacy concerns. In addition to the database security measures discussed above, these proposals include protocols protecting communications between readers and tags, such as encryption or passwords.[164] These methods would restrict access to the tag itself by requiring some measure of authentication on behalf of the scanning device. Even if a reader could get a tag to "talk," encryption would prevent the reader from understanding the message.[165] One commenter strongly urged that "[a]uthorization, authentication, and encryption for RFID . . . be developed and applied on a routine basis to ensure trustworthiness of RFID radio communications."[166]

A related technical approach discussed at the Workshop involves "blocker tags," which prevent RFID tags from communicating accurately with a reader.[167] With blocker tags, which are tags literally placed over or in close proximity to the RFID tag, consumers would be able to control which items they want blocked and when. This would allow consumers to benefit from any post-purchase applications of RFID that may develop, such as "smart" refrigerators.[168]

Finally, Workshop participants discussed the "kill switch," a feature that permanently disables at the point-of-sale an RFID tag affixed to a consumer item.[169] Such a function has been proposed as a way to provide "choice" to consumers in the context of item-level tagging.[170] However, a number of Workshop participants disputed the effectiveness of this approach. Some privacy advocates found the options of killing or blocking tags both lacking because of the burden they could impose on consumers. For example, setting up a "kill kiosk," as one retailer abroad reportedly had done,[171] contemplates that consumers first purchase an item and then deactivate an attached RFID tag. Some panelists argued that this process was cumbersome by requiring that consumers engage in two separate transactions when making a purchase. They argued that this process may dissuade consumers from exercising the option to disable tags on purchased items.[172]

Another critique of these technological "fixes" raised at the Workshop focused on their potential to reward – and thus foster – RFID use. Some participants argued that if the only method of protecting consumer privacy was to disable tags at purchase, any post-purchase benefits would accrue only to those who kept their RFID tags active.[173] As a result, these panelists suggested, consumers would be more likely to keep tags enabled.[174] Conversely, another participant argued that giving shoppers this option could drive up costs for all consumers, even those who do not object to the presence of active RFID tags on items they purchase.[175] According to this speaker, merchants would likely be reluctant to charge higher prices for consumers who elect to deactivate RFID tags prior to purchase.[176] Finally, as one commenter pointed out, the effectiveness of tag-killing technology depends on whether the presence of RFID is effectively disclosed: no consumer will seek to deactivate a tag of which she or he is unaware.[177]

VI. Conclusion

The Workshop provided Commission staff, panelists, and the public with a valuable opportunity to learn about RFID technology. In addition, the Workshop brought together RFID proponents, privacy experts, and other interested parties to discuss RFID's various current and potential applications and their implications for consumer privacy. It also highlighted proposals to address these implications and generated discussion about the merits of these different approaches.

Workshop participants generally agreed that certain RFID uses, like tagging cases and pallets of goods moving through the supply chain, may increase efficiency without jeopardizing consumer privacy. However, less consensus emerged about the implications of other potential RFID uses, such as item-level tagging of consumer products. Some panelists expressed concern about the physical characteristics of RFID devices, focusing on the small size of tags and readers and their ability to communicate even when concealed and at some distance from each other. These participants were also concerned that a third party could access information stored on RFID tags to monitor consumers surreptitiously.

Other panelists believed that privacy concerns about RFID technology were exaggerated. They doubted that RFID technology would ever have some of the capabilities that appear to raise privacy concerns, and they argued that costs will restrict the introduction of RFID into consumer environments. Finally, they asserted that RFID would not be deployed in privacy-intrusive ways, citing as evidence the range of industry self-regulatory efforts underway.

Panelists discussed a number of self-regulatory models, from RFID-specific practices to comprehensive privacy principles that implicitly incorporate RFID use. In general, these approaches incorporate disclosure of the presence of RFID technology ("notice"), providing the option to discard, remove, or disable the tags ("choice"), consumer education, and information security measures. Workshop participants agreed in particular that there is a need to protect information collected with RFID devices and stored in company databases.

Based on the Workshop discussions and comments submitted from technology experts, RFID users, privacy advocates, and consumers, Commission staff agrees that industry initiatives can play an important role in addressing privacy concerns raised by certain RFID applications. The staff believes that the goal of such programs should be transparency. For example, when a retailer provides notice to consumers about the presence of RFID tags, the notice should be clear, conspicuous, and accurate.[178] The notice should advise consumers if an RFID tag or reader is present and if the technology is being used to collect personally identifiable information about consumers. This clarity is particularly important when a disclosure concerns an unfamiliar technology, as is the case with RFID.[179] Similarly, if a company's program provides consumers with the option of removing the RFID tag, the company's practices should make that option easy to exercise by consumers. However, given the variation in RFID applications, translating these goals into concrete steps may be challenging and should occur in a way that allows flexibility to develop the best methods to address consumer privacy concerns.

Commission staff also agrees with the Workshop participants who viewed many of the potential privacy issues associated with RFID as inextricably linked to database security. The Commission has worked vigorously, through a combination of law enforcement,[180] public workshops,[181] and business education materials,[182] to ensure that companies secure consumers' personal information. As in other contexts in which personal information is collected from consumers, the staff believes that a company that uses RFID to collect such information must implement reasonable and appropriate measures to protect that data.[183] As part of implementing an information security program, the staff encourages businesses to consider whether retention of information collected from consumers through RFID or other methods is necessary or even useful.[184] The staff also recommends that any industry self-regulatory program include meaningful accountability provisions to help ensure compliance.

Another critical element of self-regulatory programs that many Workshop participants and commenters emphasized was effective consumer education.[185] The staff agrees that consumer education is a vital part of protecting consumer privacy. Industry members, privacy advocates, and government should develop education tools that inform consumers about RFID technology, how they can expect to encounter it, and what choices they have with respect to its usage in particular situations. As new applications of RFID emerge, the staff will continue to monitor these developments and consider what additional guidance or other actions are appropriate, in light of the implications of those developments for consumers.

Endnotes

1. Jo Best, *Cheat sheet: RFID*, silicon.com, Apr. 16, 2004.

2. *See, e.g.*, Allen, Texas Instruments, at 67-75. Unless otherwise noted, footnote citations are to the transcript of or comments submitted in connection with the Workshop. The Workshop transcript, specific panelist presentations, and comments are available online at http://www.ftc.gov/bcp/workshops/rfid/index.htm. Footnotes that cite to specific panelists cite to his or her last name, affiliation, and the page(s) where the referenced statement can be found in the transcript or appropriate comment. A complete list of Workshop participants can be found in Appendix A.

3. *See* Press Release, Wal-Mart, *Wal-Mart Begins Roll-Out of Electronic Product Codes in Dallas/Fort Worth Area* (Apr. 30, 2004) (available at http://www.walmartstores.com).

4. *See* Jacqueline Emigh*, More Retailers Mull RFID Mandates,* eweek, Aug. 19, 2004.

5. *See* Boone, IDC, at 226.

6. Tien, Electronic Frontier Foundation ("EFF"), at 97.

7. Press Release, FDA, *FDA Announces New Initiative to Protect the U.S. Drug Supply Chain Through the Use of Radiofrequency Identification Technology* (Nov. 15, 2004) (available at http://www.fda.gov).

8. Over the past decade, the FTC has frequently held workshops to explore emerging issues raised by new technologies. The Commission's earliest workshops on Internet-related issues were held in 1995. *See* http://www.ftc.gov/opp/global/trnscrpt.htm. More recently, the Commissions workshops have focused on such issues as wireless technologies, information security, spam, spyware, and peer-to-peer networks. For more information about each of these forums and the Commission's privacy agenda, see http://www.ftc.gov/privacy/privacyinitiatives/promises_wkshp.html.

9. This report was prepared by Julie Brof and Tracy Thorleifson of the FTC staff. It does not necessarily reflect the views of the Commission or any individual Commissioner.

10. For an explanation of how GPS operates, see http://gps.faa.gov/gpsbasics/.

11. *The EPCglobal Network: Overview of Design, Benefits, and Security* §3 (2004) (available at http://www.epcglobalinc.org).

12. *See* John Carey, *Big Brother's Passport to Pry*, Business Week, Nov. 5, 2004.

13. Image courtesy of Marks & Spencer.

14. *See* RSA Laboratories, *Technical Characteristics of RFID* (available at http://www.rsasecurity.com/rsalabs/).

15. *See Frequently Asked Questions* (available at http://www.rfidjournal.com).

16. For a discussion of these and other approaches to securing communications between RFID tags and readers, see Section V.C., *infra*.

17. Bar codes, however, are typically less expensive and have longer read ranges, provided there is line-of-sight scanning. *See* Olga Kharif*, Like It or Not, RFID IS Coming*, Business Week, Mar. 18, 2004 (noting that RFID tags now cost "at least 20 times as much" as bar codes); Parkinson,

Capgemini, at 214 (stating that "as long a bar code is visible, [it can be read] from almost a mile away with a laser scanner").

18. *See* Stafford, Marks & Spencer, at 264.

19. Image courtesy of Intel Research Seattle.

20. Image courtesy of Marks & Spencer.

21. Image courtesy of Intel Research Seattle.

22. *See Privacy FAQs* (available at http://www.rfidjournal.com); *see also* Parkinson at 213.

23. *The EPCglobal Network* §§ 5-6, *supra* note 11. As a participant at the Workshop explained, "EPCglobal is a joint venture of the Uniform Code Council and EAN International . . . . [whose] mission is simply to create global standards for the EPCglobal Network." Board, EPCglobal Public Policy Steering Committee, at 269.

24. *See* Hutchinson, EPCglobal US, at 37-38.

25. *Id.*

26. *See* http://www.ezpass.com/static/info/howit.shtml.

27. *Frequently Asked Questions*, *supra* note 15.

28. In fact, the proximity of some of those substances, particularly water or metal, may make it impossible to read an RFID tag. Engels, Auto-ID Labs, at 23-25, 27.

29. Costs are in U.S. dollars. *See Glossary of RFID Terms* (available at http://www.rfidjournal.com); *see also* Boone, IDC, at 219.

30. *See* Robert O'Harrow Jr., *Tiny Sensors That Can Track Anything*, Washington Post, Sept. 24, 2004.

31. *See* Aaron Ricadela, *Sensors Everywhere*, Information Week, Jan. 24, 2005.

32. *See Glossary of RFID Terms*, *supra* note 29.

33. *See* http://www.ezpass.com/index.html.

34. *See* Joshua Walker and Christine Spivey Overby, Forrester Research, *What You Need to Know About RFID in 2004* (available at http://www.forrester.com/ER/Research/Brief/0,1317,33298,FF.html).

35. *Id.*

36. As noted above, the theoretical distance for reading passive tags is up to 30 feet, but that longer range does not account for real-world conditions, such as interference from metals, liquids, or even wind. *See* Engels, Auto-ID Labs, at 24-25; Albers, Philips Semiconductors ("Philips"), at 35.

37. For example, Workshop attendees heard about how Marks & Spencer, a British retail chain, uses writeable tags on trays used to ship products from the company's food supplier. Each time a tray is used, the RFID tag on the outside of the tray is "written to," meaning that information about the contents of the tray for that particular shipment is loaded onto the chip. Stafford, Marks & Spencer, at 262-63.

38. The EPCglobal Network is an example of such a system. *See supra* note 11.

39. *Id.*; Allen, Texas Instruments, at 73.

40. Allen, Texas Instruments, at 73; *see also* Laurie Sullivan, *How RFID Will Help Mommy Find Johnny*, InformationWeek, Sept. 15, 2004.

41. Allen, Texas Instruments, at 68; *see also* Albers, Philips, at 32-33.

42. According to a Workshop participant, seven million U.S. consumers currently use Speedpass. Allen, Texas Instruments, at 70. In addition to payment mechanisms like Speedpass, major credit card companies are developing "contactless smart cards" to facilitate purchases at a variety of venues. Albers, Philips, at 32 (noting that MasterCard, Visa, and American Express are developing such cards). One recent example is the acceptance of MasterCard's "PayPass" at McDonald's. *McDonald's to Roll Out Contactless Payments in USA*, UsingRFID.com, Aug. 30, 2004.

43. *See, e.g.,* http://www.ezpass.com/index.html. A recently announced initiative by the Orlando/ Orange County Expressway Authority ("OOCEA") in Florida will take this concept even further. OOCEA plans to install roadside RFID readers to gather data from about 1 million RFID tags attached to cars. The program is designed to determine accurate travel times and improve traffic flow. After the information is encrypted and stripped of any personal identifiers, drivers will be able to access it from signs along the highway, by phone, and eventually through a Web site. Claire Swedberg, *RFID Drives Highway Traffic Reports*, RFID Journal, Nov. 17, 2004.

44. Sarah Lacy, *Inching Toward the RFID Revolution*, Business Week, Aug. 31, 2004.

45. Hughes, Procter & Gamble ("P&G"), at 167.

46. *See* Julie Hutto and Robert D. Atkinson, PPI, *Radio Frequency Identification: Little Devices Making Big Waves,* at 3-4 (Oct. 2004) (arguing that retailers' costs savings attributable to RFID would be quickly passed on to consumers because of "fierce competition"). However, a number of panelists at the Workshop suggested that the adoption of RFID by retailers would not necessarily result in lower prices for consumers, at least not in the near future. *See* Hughes, P&G, at 196; Duncan, National Retail Federation ("NRF"), at 196-97.

47. Wood, Retail Industry Leaders Association ("RILA"), at 52-53.

48. *Id.* According to the Grocery Manufacturers of America, an estimated 8 percent of the time consumers can't find what they want on retailers' shelves, and that number can climb to 15 percent during a product promotion. Barnaby J. Feder, *RFID: Simple Concept Haunted by Daunting Complexity*, N.Y. Times, Nov. 21, 2004.

49. Wood, RILA, at 54; Langford, Wal-Mart, at 62-64. According to Langford, Wal-Mart intends to monitor shipments as they leave suppliers, which will provide additional visibility early in the supply chain, not just when products arrive at a Wal-Mart distribution center.

50. Langford, Wal-Mart, at 62-63. As explained above, unlike bar codes, RFID tags do not require line-of-sight or individual scanning to be read.

51. This panelist explained how RFID could reduce the need for retailers to order "safety stock," which are the additional goods purchased in order to avoid having a shortage of necessary items. Safety stock sits unsold on the shelf, and is thus a source of inefficiency. Wood, RILA, at 53.

52. Wood, RILA, at 54; *see also* Langford, Wal-Mart, at 67; Grocery Manufacturers of America ("GMA"), Comment, at 3.

53. Woods, RILA, at 53.

54. Boone, IDC, at 218-19. *See also* Stafford, Marks & Spencer, at 264 (asserting that "[t]he business case for using RFID tags is entirely about the speed of read").

55. Wood, RILA, at 55.

56. *Id.* at 54-55 (explaining that RFID will help ensure that consumers don't "buy aspirin and then have it expire on [them] in three months"); *see also* GMA, Comment, at 3.

57. Tien, EFF, at 96-98; *see generally* Mulligan, Samuelson Law, Technology, and Public Policy Clinic ("Samuelson Clinic"), at 152-162. Another recent development that has emerged since the Workshop concerns announcements by some American schools to use RFID-tagged identification cards to monitor student bus travel and/or attendance. *See* Matt Richel, *In Texas, 28,000 Students Test an Electronic Eye*, N.Y. Times, Nov. 17, 2004.

58. DoD is also already using active RFID tags to track materiel in the supply chain and to identify the location of such items. William Jackson, *Defense Calls Shotgun on RFID*, Government Computer News, Apr. 19, 2004, at 10.

59. *See* Tien, EFF, Comment, at Table 1. As one participant explained, library RFID systems are not using an open-source, EPC-type network, but instead are designed to be specific to each institution. Each library's numbering and standards are different, so two libraries would not be able to interpret each other's coding system, making it more difficult for a third party to "break the code" and surreptitiously trace a consumer's reading habits. *See* Mulligan, Samuelson Clinic, at 158.

60. *See generally* Rudolf, FDA, at 82-94. The FDA issued a report calling for RFID use in the pharmaceutical supply chain, *Combating Counterfeit Drugs*, in February 2004.

61. *See* Press Release, FDA, *FDA Announces New Initiative to Protect the U.S. Drug Supply Chain Through the Use of Radiofrequency Identification Technology* (Nov. 15, 2004) (available at http://www.fda.gov/bbs/topics/news/2004/NEW01133.html).

62. *See* Gardiner Harris, *Tiny Antennas to Keep Tabs on U.S. Drugs*, N.Y. Times, Nov. 15, 2004.

63. Rudolf, FDA, at 85; *see also* Healthcare Distribution Management Association ("HDMA"), Comment, at 2 (stating that RFID "will serve as a barrier to entry of unsafe products in the supply chain by establishing a secure electronic means through which every unit of medication can be verified, in terms of its source and path through the supply chain").

64. Rudolf, FDA, at 86-87; FDA, Comment, at 1.

65. Sand, DHS, at 105.

66. Las Vegas McCarran International Airport was the first airport to use RFID-embedded baggage tags. RFID tags are embedded in paper identification tags attached to each piece of luggage. *Radio ID Tags to Debut at Las Vegas Airport*, Federal Times, Dec. 15, 2003. The Transportation Security Administration ("TSA") has since announced the selection of additional airports that will deploy RFID as part of the agency's "Access Control Pilot Program." TSA, Press Release, *TSA Announces Two More Airports Now in Access Control Pilot Program*, Aug. 25, 2004 (available at http://www.tsa.gov).

67. In 2003, Delta Airlines announced a pilot program using RFID to track and trace passenger luggage. The trial, implemented in conjunction with TSA, embedded RFID tags in paper baggage

tags, which were read at key points throughout the travel process. *Delta Takes RFID Under its Wing*, RFID Journal, June 20, 2003.

68. Aliya Sternstein, *Land-ho for US-VISIT*, Federal Computer Week, Nov. 9, 2004. For more information, see DHS, *Fact Sheet: U.S. Land Borders,* at 3 (available at http://www.dhs.gov/us-visit).

69. Sand, DHS, at 106. An analogous program, the "Free and Secure Trade Program" ("FAST"), reportedly also will use RFID to facilitate border crossings by commercial truck drivers who routinely traverse the U.S.-Canadian border. RFID-embedded stickers on truck windshields and identification cards for truck drivers will expedite such crossings and enhance border security. *See* Press Release, DHS, *United States - Canada Free and Secure Trade Program*, Sept. 9, 2002 (available at http://www.dhs.gov); *see also eGo Tags to Extend US Border Security Programme*, UsingRFID.com, Dec. 19, 2003.

70. *See id.* at 110-11. Some privacy advocates have expressed concerns over the apparent absence of privacy protections for the use of RFID chips in passports, which could potentially permit the embedded data to be "skimmed" surreptitiously. Matthew L. Wald, *New High-Tech Passports Raise Snooping Concerns*, N.Y. Times, Nov. 26, 2004. The U.S. State Department, which is responsible for issuing the new passports, has argued that the need for "global interoperability" in reading them precludes measures like data encryption. In addition, DHS asserts that some simple measures, such as the addition of metal fibers to the cover, could prevent an unopened passport from being scanned. Leslie Miller, *U.S. Opposes Passport Privacy Protections*, Washington Post, Nov. 28, 2004.

71. *See* Fishkin, Intel, at 77, 81. In addition, two medical devices using RFID recently have been approved. The "VeriChip Health Information Microtransponder" is an RFID tag designed for human use; it can be embedded with a unique identification number and implanted below the skin. Doctors or hospital staff can scan individuals who have agreed to be implanted with the VeriChip, and the embedded code can be used to access a database containing the patient's identity and health information. *See* Josh McHugh, *A Chip in Your Shoulder: Should I Get an RFID Implant?*, Slate, Nov. 10, 2004. Another device, the "SurgiChip Tag Surgical Marker System," will use RFID technology to assist surgeons during operations. RFID tags bearing a patient's name and surgical site will be affixed to the patient at the proper spot and scanned by the surgeon prior to performing a procedure. Lee Bowman, *Surgeons Get High-Tech Help to Cut Errors*, Seattle Post-Intelligencer, Nov. 20, 2004. The SurgiChip was approved for sale in November 2004, following approval of the VeriChip the previous month.

72. *See* Fishkin, Intel, at 75-82.

73. Intel is also researching the feasability of integrating a tag into a bracelet, which would be more user-friendly. Fishkin, Intel, at 80. The reader would track what tagged objects the senior picked up and wirelessly communicate that information to a computer program. The program could infer from a set of specific actions (for example, picking up a cup, a saucer, and a kettle) what task the senior is engaged in (for example, making tea). *Id.*; *see also* Kristi Heim, *A Hand in the Future*, Seattle Times, Dec. 9, 2004.

74. Fishkin, Intel, at 78-80.

75. Albrecht, Consumers Against Supermarket Privacy Invasion and Numbering ("CASPIAN"), at 236. In addition to using RFID to track inventory through the supply chain, Metro reportedly has also used RFID tags on certain consumer products in their model "Future Store" in Rheinberg, Germany. The chain had also developed RFID-embedded customer loyalty cards, an experiment

it publically abandoned in early 2004. *Future Store Keeps RFID Except in Loyalty Cards*, UsingRFID, March 5, 2004.

76. Livingston, Livingston & Co., at 180.

77. Boone, IDC, at 219.

78. *Id.* Five cents is often cited as the tipping point, because it makes the tagging of inexpensive items economically feasible. *See, e.g.,* Ginsburg, Accenture, at 46.

79. Wood, RILA, at 58.

80. Boone, IDC, at 220.

81. The survey discussed at the Workshop, "RFID and Consumers: Understanding Their Mindset," was commissioned by Capgemini and the National Retail Federation and is available at http://www.nrf.com/download/NewRFID_NRF.pdf. Unless otherwise noted, references to survey results concern this study.

82. The unfamiliarity with the concept of RFID extended even to those consumers who might be using it. For example, eight out of ten survey respondents did not know that the ExxonMobil Speedpass and the E-ZPass employ RFID technology.

83. Other pre-programmed benefits consumers were asked to rank included improved security of prescription drugs, faster and more accurate product recalls, improved price accuracy, faster checkout times, and reduced out-of-stocks.

84. Consumer comments are available at http://www.ftc.gov/bcp/workshops/rfid/index.htm.

85. BIGresearch and Artafact LLC released the results of their joint study, "RFID Consumer Buzz," in October 2004. A summary is available at http://www.bigresearch.com.

86. The RFID Consumer Buzz survey broke respondents into two categories: "RFID-aware" and "RFID non-aware" consumers. Interviewers described how RFID works to the latter group prior to asking them about perceived benefits and concerns associated with the technology.

87. According to an Artafact spokesperson, "The people [who] were aware of RFID were more practical about balancing the positives and the negatives. Those who were not aware seemed to be surprised to learn about the technology, and they gravitated more toward the potential negative impacts of RFID. We concluded from that that it's better to inform people about the positive applications than to wait for them to discover the technology on their own." Mark Roberti, *Consumer Awareness of RFID Grows*, RFID Journal, Oct. 22, 2004.

88. *See* Albrecht, CASPIAN, at 228-29 (discussing a hypothetical manufacturer's internal RFID program); Stafford, Marks & Spencer, at 264.

89. Privacy advocates at the Workshop collectively called for RFID to be subjected to a neutral, comprehensive technology assessment. For a discussion of this and other requests by these advocates, see *infra* Section V.B.

90. Givens, Privacy Rights Clearinghouse ("PRC") at 145; CASPIAN, PRC, et al., *Position Statement on the Use of RFID on Consumer Products ("Privacy Position Statement")*, Comment, at 2. This capability distinguishes EPCs from typical bar codes, which use generic identifiers.

91. *Id.* For example, using RFID devices to track people (such as students) or their automobiles (as with E-ZPasses) could generate precise and personally identifiable data about their movements,

raising privacy concerns. As one ninth grader in the Texas school system that reportedly plans to use RFID explained, "Something about the school wanting to know the exact place and time [of my whereabouts] makes me feel like an animal." Matt Richtel, *In Texas, 28,000 Students Test an Electronic Eye,* N.Y. Times, Nov. 17, 2004.

92. *See, e.g.,* Givens, PRC, at 145; Parkinson, Capgemini, at 213-14.

93. Fishkin, Intel, at 76. He also stated that he had recently seen a reader the size of a U.S. dime, but explained that the scanning range for such small readers would be less than an inch. These readers would be appropriate for hospital use, for example; they can be integrated into medical equipment "to make sure that when you stick RFID tagged object A into . . . RFID reader receptacle B, you did the right thing." *Id.* at 78.

94. *See* Albrecht, CASPIAN, at 235.

95. *See id.* at 232; Givens, PRC, at 145.

96. Parkinson, Capgemini, at 213-14.

97. *Privacy Position Statement* at 2.

98. *See* Tien, EFF, at 96; Mulligan, Samuelson Clinic, at 156.

99. *See, e.g.,* Juels, RSA Labs, at 311. This access depends on whether RFID devices are interoperable. Currently, "existing RFID systems use proprietary technology, which means that if company A puts an RFID tag on a product, it can't be read by company B unless they both use the same vendor." *See Frequently Asked Questions*, *supra* note 15. This limitation may change, however, with the recent announcement by EPCglobal approving the second-generation EPC specification. The so-called Gen 2 standard will allow for global interoperability of EPC systems, although it is unclear when Gen 2-compliant products will be introduced or whether the initial round of these products will be interoperable. *See* Jonathan Collins, *What's Next for Gen 2?*, RFID Journal, Dec. 27, 2004.

100. Albrecht, CASPIAN, at 231.

101. *See id.*; *see also* Atkinson, Progressive Policy Institute ("PPI"), at 291 (explaining that "[e]very time I use a credit card, I link product purchases to [personally identifiable information]. We've been doing it for 30 years"). *Cf.* Constance L. Hays, *What Wal-Mart Knows About Customers' Habits*, N.Y. Times, Nov. 14, 2004 (describing the tremendous amount of customer data Wal-Mart maintains, but claims it currently does not use to track individuals' purchases).

102. Albrecht, CASPIAN, at 231.

103. *See Privacy Position Statement* at 2.

104. Mulligan, Samuelson Clinic, at 157 (asserting that such profiling may even be more "troublesome" where the tagged item is a book or other type of information good).

105. Albrecht, CASPIAN, at 239.

106. *Id.* at 239-40.

107. *E.g.,* Hughes, Procter & Gamble ("P&G"), at 173 (asserting that P&G is "not doing item-level testing"); Wood, RILA, at 60 ("We see a little bit of testing going on in the item level. We do not see widespread item adoption . . . or use for at least ten years").

108. Boone, IDC*,* at 222-23; *see also* Maxwell, International Public Policy Advisory Councils, Auto-ID Labs and EPCglobal, at 257-58 (noting the alignment between the interests of retailers and consumers in protecting data generated by RFID systems).

109. Waldo, Sun Microsystems ("Sun"), at 248 (explaining that if a reader is trying to "read[] from very far away, you're not only going to get your stuff read, you're going to get a tan," because of the powerful amount of energy required).

110. *Id.* at 249-50.

111. Stafford, Marks & Spencer, at 313 (advising the public to "[b]e clear, there isn't a business case about gathering customer information through RFID").

112. A number of technological proposals to resolve privacy issues are addressed in Section V.C., *infra*.

113. As one commentator has observed: "RFID is one data-gathering technology among many. And people should be worried about how data related to them gets handled and regulated. That's much more important than how it's gathered, because it will be gathered one way or another." Thomas Claburn, *RFID Is Not The Real Issue*, InformationWeek, Sept, 13, 2004.

114. Hutchinson, EPCglobal US, at 26. However, outside of the EPC and supply chain context, privacy concerns center on the security of communication between tags and readers. For example, the proposed biometric passports, *see supra* note 70, have been criticized as having inadequate privacy protections. This lack of security could enable the rogue scanning of biometric data embedded on RFID chips in passports. Under these circumstances, access to a database would not be necessary to interpret that information.

115. Hutchinson, EPCglobal US, at 38; *see also The EPCglobal Network* §7.1, *supra* note 11.

116. Kim Hargraves and Steven Shafer, Microsoft, *RFID Privacy: The Microsoft Perspective* (2004) ("Microsoft Comment").

117. *Id.* at 6; *see also* discussion, *supra* note 99. In this situation, a product supplier may share access with its distributor partners to a database that holds information about its RFID-tagged goods, so that each entity can track those items.

118. *Id.*; *see also The EPCglobal Network* §§ 7.3-7.4, *supra* note 11. EPCglobal argues that security concerns about both the Object Naming Service and network information are not unique to the EPC system: "As with all corporate information, companies have a vested interest in the security of their information and systems."

119. Microsoft, Comment at 10.

120. *Id.* Microsoft advocates that where personally identifiable information about consumers is collected, via RFID or in other contexts, the "widely accepted concept of Fair Information Practices" should be followed. *Id.* at 14-15. Microsoft's comment discusses in some detail these and other consumer privacy guidelines for industry. *See id.*

121. Hutchinson, EPCglobal US, at 38.

122. *See* Givens, PRC, at 145; Mulligan, Samuelson Clinic, at 159; Waldo, Sun, at 253-54.

123. *See* Bruening, Center for Democracy & Technology ("CDT"), at 312 (arguing that coupling computing power with information generated by RFID allows that data "to be shared and collated

and mined so efficiently, and . . . that because of that power and those rich dossiers that we can potentially create, our concerns about who has access to that become greater").

124. *E.g.,* Waldo, Sun, at 253-54 (noting that "were I a mad scientist . . . I think it would be great thing to get people all stirred up about RFID privacy so that they would be worried about that, and I could go off and invade the real privacy on the databases myself").

125. *See* Maxwell, International Public Policy Advisory Councils, Auto-ID Labs and EPCglobal, at 260; Bruening, CDT, at 285-86.

126. This panel focused largely on the privacy challenges facing private industry. The costs and benefits of RFID deployment by government, including current and proposed uses by the Department of Homeland Security, raise issues not addressed in depth at the Workshop or in comments submitted to the Commission.

127. The Guidelines are posted at http://www.epcglobalinc.org/consumer/, under the public policy section of the EPCglobal Inc. Web site.

128. Board, EPCglobal, at 271-72. EPCglobal currently has over 400 members.

129. *Id.* at 272.

130. Board, EPCglobal, at 272 and presentation slide. More information about the template label is available on the EPCglobal Web site, along with explanatory information for consumers about RFID technology. *See* http://www.epcglobalinc.org/consumer/.

131. Board, EPCglobal, at 272 and presentation slide.

132. The significance of this provision and the protection it provides consumers obviously depends on the existence and rigor of applicable privacy laws or regulations.

133. All quoted items are excerpts from the EPCglobal Guidelines, *supra* note 127.

134. The Guidelines provide that "EPCglobal will monitor the proper use of these Guidelines," but details concerning enforcement or accountability mechanisms have not yet been announced.

135. Board, EPCglobal, at 272; *see also* GMA, Comment, at 5 (stating that "[i]n January 2004, the GMA Board of Directors formally adopted privacy guidelines established by EPCglobal"). In addition, some industry members have endorsed self-regulatory principles similar to those embodied by the EPCglobal Guidelines. *See, e.g.*, NRF, Comment; Microsoft, Comment, at 14-15. Another example is the 1,500-member Food Marketing Institute, which added RFID-specific provisions to its "Policy Statement on Consumer Privacy" in May 2004. In addition to calling for notice, choice, access, and security of consumer data, the FMI statement advocates legislation prohibiting the unauthorized access, interception, or receipt of an "EPC signal" (i.e., barring the rogue scanning of RFID tags). *See* http://fmi.org/consumer/privpolicy.htm. Commission staff will continue to monitor compliance with the EPCglobal Guidelines and other industry self-regulatory standards.

136. Board, EPCglobal, at 272; Langford, Wal-Mart, at 65-66. Wal-Mart's RFID announcement calls for its top 100 suppliers to place RFID tags on cases and pallets shipped to a regional distribution center in Texas. Readers will be installed at the dock doors of seven stores in the Dallas-Ft. Worth metropolitan area in order to track tagged cases or packages of goods. No readers are placed on store floors. Other company stores in the distribution center's region, which covers North Texas and parts of Oklahoma, may receive RFID-tagged cases and pallets, but no readers

will be installed there as part of the pilot program. For more information about Wal-Mart's RFID plans, see the "Supplier Information" section of http://www.walmartstores.com.

137. Wal-Mart's shelf-talker is attached as Appendix B.

138. *See* Langford, Wal-Mart, at 66.

139. A list of current P&G trials using EPC technology is available at http://www.pg.com/company/our_commitment/privacy_policy/index.jhtml.

140. P&G, Comment; *see also* http://www.pg.com/company/our_commitment/privacy_policy/index.jhtml.

141. Hughes, P&G, at 172. However, some panelists asserted that retailers currently use bar code data to link customer identity to their purchases. Albrecht, CASPIAN, at 231; *see also* Atkinson, PPI, at 291.

142. *See* Stafford, Marks & Spencer, at 265.

143. Prior to implementing their program, company officials met with key privacy organizations in an effort to accommodate their concerns. *See* Marks & Spencer, *Corporate Social Responsibility, Issue Two: Responsible Use of Technology* (available at http://www2.marksandspencer.com/thecompany/).

144. Consumers may detach the tags themselves post-purchase or may request that a cashier do so. The tags are not required for return, so may be discarded by consumers without further consideration. For a picture of what an Intelligent Label looks like, see Figure B, *supra*.

145. Stafford, Marks & Spencer, at 266-68. The leaflet is attached as Appendix C.

146. Specifically, privacy advocates called for RFID users to "make public their policies and practices involving the use and maintenance of RFID systems." Further there should be no "secret databases" or "tag-reading in secret." *Privacy Position Statement* at 3.

147. *See id.*; Laurant, Electronic Privacy Information Center ("EPIC"), at 278.

148. Laurant, EPIC, at 278.

149. Givens, PRC, at 211.

150. *See id.*

151. The *Privacy Position Statement*, which forty-five consumer and privacy organizations have signed, endorses the need for such an assessment. Workshop participants representing some of these groups reiterated this recommendation. *See* Givens, PRC, at 150-51, Laurant, EPIC, at 279; Bruening, CDT, at 282-83.

152. Givens, PRC, at 150-51. For example, RFID tags could be used effectively for recycling purposes without containing unique identifiers; instead, the chips could be encoded to communicate only the presence of certain toxins that recyclable materials may contain. A comment from a consumer made an analogous suggestion, recommending that tollway transponders (such as E-ZPass), be sold like phone cards in stores, where they could be purchased with cash and used anonymously. *See* Greenberg, Comment.

153. *Privacy Position Statement* at 3-4.

154. *See* Tien, EFF, at 100-01; Laurant, EPIC, at 279. In addition, although Workshop participants did not discuss state legislation, a number of bills have been introduced across the country, including California, Maryland, Massachusetts, and Utah. *See* Claire Swedberg, *States Move on RFID Privacy Issue,* RFID Journal, Apr. 30, 2004; Thomas Claburn, *Privacy Fears Create Roadblocks for RFID*, InformationWeek, Mar. 8, 2004. These proposals, which were not enacted, would have required notice and other measures in connection with a retailer's use of RFID on individual consumer items. Some observers believe that these or similar proposals are likely to resurface in next year's legislative sessions. *See* Kristi Heim, *Microchips in People, Packaging, and Pets Raise Privacy Concerns*, Seattle Times, Oct. 18, 2004 (citing interest among Washington State legislators in addressing privacy concerns raised by RFID use).

155. Laurant, EPIC, at 279; *see also* EPIC, Comment, at 14.

156. Laurant, EPIC, at 279 (noting the application of European Union privacy directives to personal data collected via RFID and recently adopted RFID-specific guidelines in Italy and Japan).

157. *Privacy Position Statement* at 3.

158. *See id.*

159. *See* Laurant, EPIC, at 277; *see also* EPIC, Comment, at 18 (noting the need for accountability as part of comprehensive guidelines for RFID users).

160. *See* Duncan, NRF, at 143; Atkinson, PPI, at 293.

161. Maxwell, International Public Policy Advisory Councils, at 311.

162. MacLeod, GMA, at 177-79, 193-94.

163. *Id.*; *see also* Duncan, NRF, at 141-43 and Comment (discussing how existing self-regulatory practices could effectively address consumer privacy concerns raised by retailers' RFID use).

164. *See* Albers, Philips, at 30. Limiting the ability of tags to "talk" to readers could address the concern that unidentified third parties with access to readers could surreptitiously scan consumers and learn about tagged items they were carrying or wearing.

165. *Id.*

166. Microsoft, Comment, at 13.

167. As one panelist explained, blocker tags work by essentially "spamming" readers by confusing them with so many announcements from chips that the reader is effectively overwhelmed. Juels, RSA Labs, at 300-01. Because of the potential for blocker tag abuse by shoplifters trying to evade a store's security system, RSA Labs has recently unveiled a modified approach. RSA's "soft blocker" technology would allow consumers to exercise some control over the status of RFID tags on items they purchase. Consumers could swipe their loyalty cards at the point of sale, which would link to data about their individual privacy preferences. This information would instruct the "privacy bit" – a portion of the code embedded on an RFID tag – to, for example, ignore certain readers. This arrangement would thus allow tags to remain active for certain post-sale purposes, with the opportunity for consumers to exercise some choice about third-party access to tags on their purchased goods. George V. Hulme and Thomas Claburn, *RFID's Security Challenge*, Information Week, Nov. 15, 2004.

168. Juels, RSA Labs*,* at 301. According to one panelist, smart refrigerators could offer consumers a number of conveniences, such as identifying expired items and generating shopping lists. *See*

Duncan, NRF, at 204; *see also Can RFID Save the Planet?*, RFID Journal, Aug. 23, 2004 (describing a hypothetical RFID-enabled refrigerator that could "recommend a menu based on seasonal organic food grown locally"). Other potential post-purchase consumer benefits of RFID that have been touted include faster and more accurate product recalls, such as defective tires or perishable items, and receipt-free returns. *See* Jim Harper, *RFID Tags and Privacy: How Bar-Codes-On-Steroids Are Really a 98-Lb. Weakling* (Competitive Enterprise Institute, On Point No. 89, June 21, 2004).

169. *See* Albers, Philips, at 35; Givens, PRC, at 146.

170. *See, e.g.*, Susan Fogarty, *Don't Let Ignorance Block RFID*, SearchSAP.com, Mar. 16, 2004.

171. *See* Mark Roberti, *Roll Up Your Sleeves*, RFID Journal, Jan. 19, 2004 (describing Germany's Metro Group's RFID deployment). Technically, Metro may offer consumers the option to anonymize, rather than actually disable, RFID tags on purchased items. Josh McHugh, *Attention, Shoppers: You Can Now Speed Straight Through Checkout Lines!*," WIRED Magazine, July 2004.

172. Givens, PRC, at 146; Juels, RSA Labs, at 299 (observing that "if you give consumers a choice between convenience or lack thereof – and having RFID will be convenient – of course, they'll choose the convenient option").

173. For example, in the future, consumers may use RFID-enhanced home appliances or benefit from a faster and more accurate product recall system that relies on RFID. *See supra* note 168.

174. *See Privacy Position Statement* at 8.

175. *See* Atkinson, PPI, at 292.

176. *See id.*

177. Gal Eschet, *A New Challenge to Privacy Management: Adapting Fair Information Practices to Radio Frequency Identification Technology* (May 2004), at 27.

178. These considerations are consistent with what the Commission has recommended in other contexts, such as online advertising. *See* Federal Trade Commission, *Dot Com Disclosures: Information About Online Advertising* 4-5 (2000), available at http://www.ftc.gov/bcp/conline/pubs/buspubs/dotcom/index.html (advising that "disclosures must be communicated effectively so that consumers are likely to notice and understand them").

179. As one Workshop participant warned, notices can be ineffective or even counterproductive if they simply serve as marketing materials championing the benefits of a particular technology. *See* Givens, PRC, at 211.

180. The Commission has sought to secure consumer information through enforcement of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits deceptive or unfair acts or practices in or affecting commerce, and the Safeguards Rule, 16 C.F.R. Part 314, which requires financial institutions to have reasonable policies and procedures to ensure the security and confidentiality of customer information. *See Sunbelt Lending Serv., Inc.,* FTC Dkt. No. C-4129 (File No. 042-3153 filed Jan. 3, 2005) (enforcing the Safeguards Rule); *Petco Animal Supplies, Inc*. (File No. 032-3221 placed on the public record Nov. 17, 2004) (enforcing Section 5); *Nationwide Mortgage Group, Inc.,* FTC Dkt. No. C-9319 (File No. 042-3104 placed on the public record March 4, 2005) (enforcing the Safeguards Rule); *Gateway Learning Corp.*, FTC Dkt. No. C-4120 (File No. 042-3047 filed Sept. 10, 2004) (enforcing Section 5); *MTS d/b/a*

Tower Records/Books/Video, FTC Dkt. No. C-4110 (File No. 032-3209 filed June 2, 2004) (enforcing Section 5); *Guess.com, Inc.*, FTC Dkt. No. C-4091 (File No. 022-3260 filed Aug. 5, 2003) (enforcing Section 5); *Microsoft Corp.*, FTC Dkt. No. C-4069 (File No. 012-3240 filed Dec. 25, 2002) (enforcing Section 5); *Eli Lilly and Co.*, FTC Dkt. No. C-4047 (File No. 012-3214 filed May 10, 2002) (enforcing Section 5).

181. Most recently, the Commission held a workshop on "Technologies for Protecting Personal Information," a two-part forum held in May and June 2003. Additional information about that workshop and others on related topics is available at http://www.ftc.gov/privacy/privacyinitiatives/promises_wkshp.html.

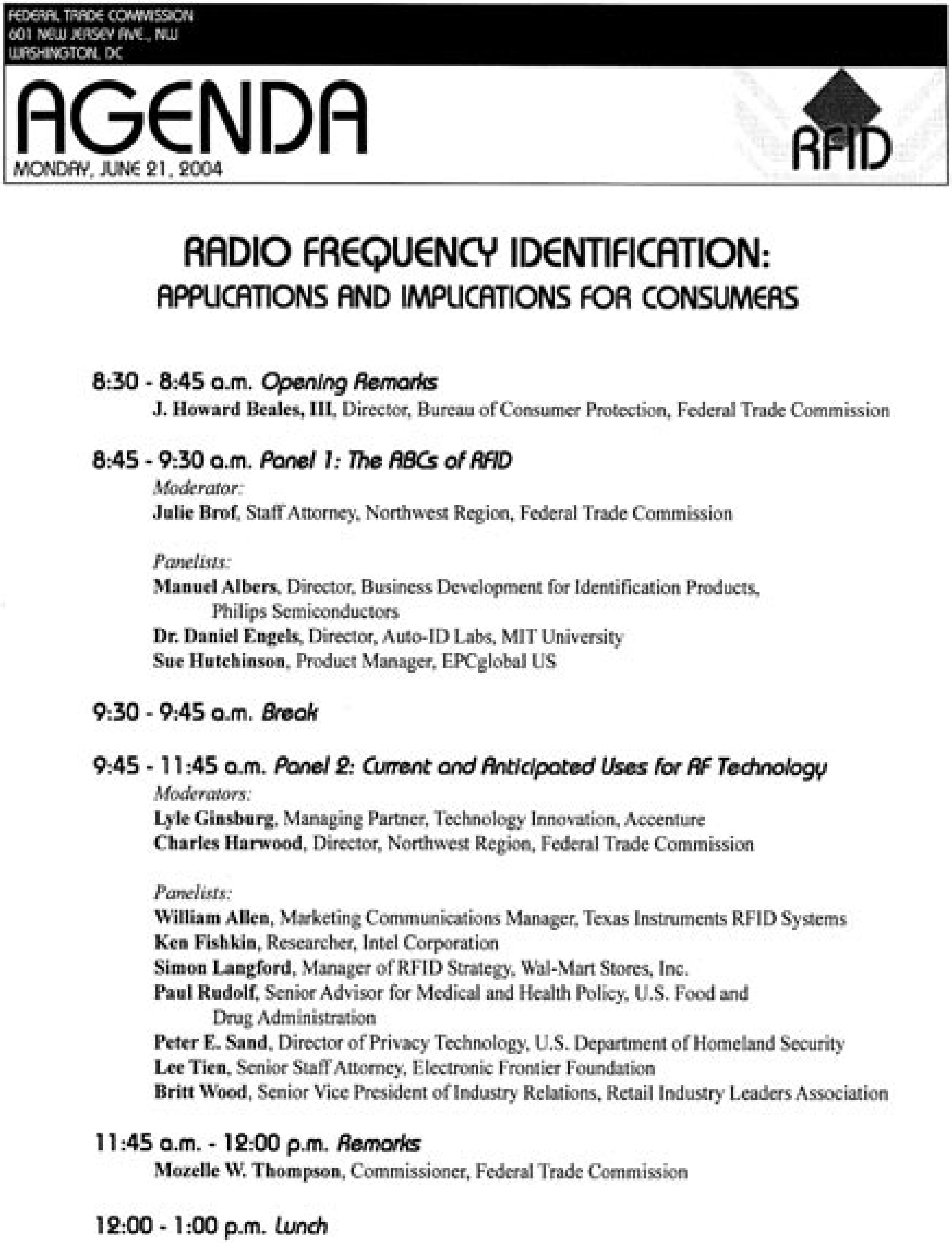
182. *See, e.g.,* Federal Trade Commission, *Information Compromise and the Risk of Identity Theft: Guidance for Your Business* (2004) (available at http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.pdf).

183. The appropriateness of such security measures will depend on the sensitivity of the information collected and the nature of the company's business. *See, e.g.*, *Petco, supra* note 180 (resolving Commission claims that Petco had violated its own privacy policy – and federal law – by failing to take reasonable or appropriate measures to prevent commonly known attacks by hackers).

184. According to one Workshop participant, at this point no business case exists to collect customer data through RFID devices. Stafford, Marks & Spencer, at 313.

185. As one Workshop panelist representing RFID users explained, it is in companies' "best interests to keep [consumers] informed, because if we do anything that could possibly make our customers uncomfortable, we will lose their business." Wood, RILA, at 60.

Appendix A: Workshop Agenda



FEDERAL TRADE COMMISSION
601 NEW JERSEY AVE., NW
WASHINGTON, DC

AGENDA

MONDAY, JUNE 21, 2004

RADIO FREQUENCY IDENTIFICATION:
APPLICATIONS AND IMPLICATIONS FOR CONSUMERS

8:30 - 8:45 a.m. ***Opening Remarks***

J. Howard Beales, III, Director, Bureau of Consumer Protection, Federal Trade Commission

8:45 - 9:30 a.m. ***Panel 1: The ABCs of RFID***

Moderator:
Julie Brof, Staff Attorney, Northwest Region, Federal Trade Commission

Panelists:
Manuel Albers, Director, Business Development for Identification Products, Philips Semiconductors
Dr. Daniel Engels, Director, Auto-ID Labs, MIT University
Sue Hutchinson, Product Manager, EPCglobal US

9:30 - 9:45 a.m. ***Break***

9:45 - 11:45 a.m. ***Panel 2: Current and Anticipated Uses for RF Technology***

Moderators:
Lyle Ginsburg, Managing Partner, Technology Innovation, Accenture
Charles Harwood, Director, Northwest Region, Federal Trade Commission

Panelists:
William Allen, Marketing Communications Manager, Texas Instruments RFID Systems
Ken Fishkin, Researcher, Intel Corporation
Simon Langford, Manager of RFID Strategy, Wal-Mart Stores, Inc.
Paul Rudolf, Senior Advisor for Medical and Health Policy, U.S. Food and Drug Administration
Peter E. Sand, Director of Privacy Technology, U.S. Department of Homeland Security
Lee Tien, Senior Staff Attorney, Electronic Frontier Foundation
Britt Wood, Senior Vice President of Industry Relations, Retail Industry Leaders Association

11:45 a.m. - 12:00 p.m. ***Remarks***

Mozelle W. Thompson, Commissioner, Federal Trade Commission

12:00 - 1:00 p.m. ***Lunch***

1:00 - 3:00 p.m. *Panel 3: Implications of RFID Use for Consumers*

Moderators:

Ellen Finn, Staff Attorney, Division of Financial Practices, Federal Trade Commission
Frederick C. (Ted) Livingston, Privacy Consultant

Panelists:

Mallory Duncan, Senior Vice President and General Counsel, National Retail Federation
Beth Givens, Director, Privacy Rights Clearinghouse
Sandra (Sandy) Hughes, Global Privacy Executive, Procter & Gamble
William MacLeod, Senior Partner, Collier Shannon Scott and Counsel, Grocery Manufacturers of America
Deirdre Mulligan, Director, Samuelson Law, Technology and Public Policy Clinic, Boalt Hall School of Law
John Parkinson, Vice President and Chief Technologist, Capgemini
Dan White, Technical Evangelist - RFID, New Technologies Retail Solutions Division, NCR

3:00 - 3:15 p.m. *Break*

3:15 - 4:00 p.m. *Panel 4: Looking Ahead: Competing Visions of the Future of RFID*

Moderator:

Julie Brof, Staff Attorney, Northwest Region, Federal Trade Commission

Presenters:

Katherine Albrecht, Founder and Director, CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering)
Christopher Boone, Program Manager, IDC
Jim Waldo, Distinguished Engineer, Sun Microsystems

4:00 - 5:30 p.m. Panel 5: *Meeting the Challenge: Best Practices and Principles*

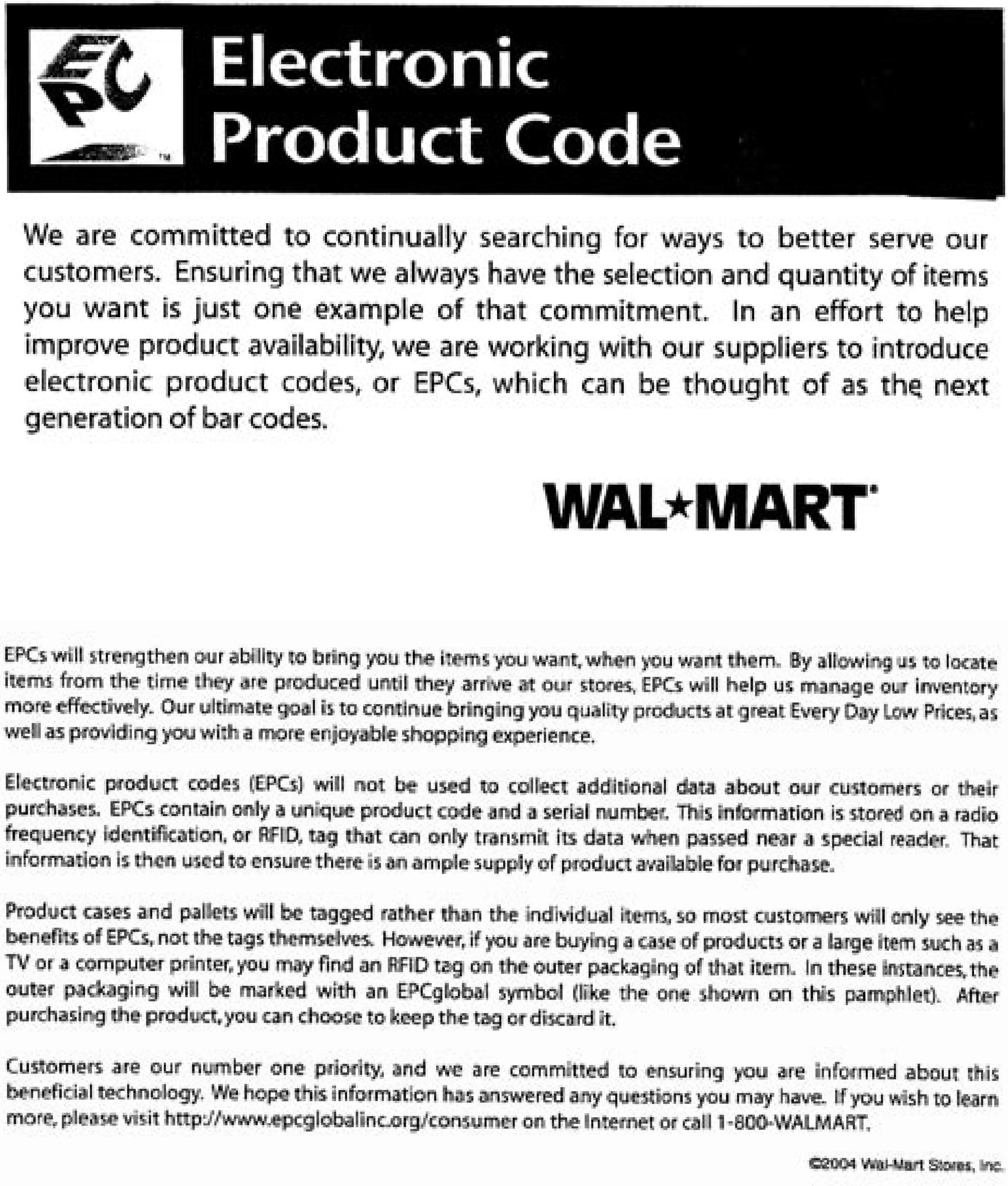
Moderators:

Elliot Maxwell, Fellow, Center for the Study of American Government, Johns Hopkins; Distinguished Research Fellow, eBusiness Research Center, Pennsylvania State University
Tracy Thorleifson, Staff Attorney, Northwest Region, Federal Trade Commission

Panelists:

Dr. Robert Atkinson, Vice President and Director, Technology & New Economy Project, Progressive Policy Institute
Elizabeth Board, Executive Director, EPCglobal Public Policy Steering Committee
Paula Bruening, Staff Counsel, Center for Democracy & Technology
Dr. Ari Juels, Principal Research Scientist, RSA Labs
Cedric Laurant, Policy Counsel, Electronic Privacy Information Center
James Stafford, Head of RFID, Marks & Spencer

Appendix B: Wal-Mart EPC "Shelf-Talker"



Electronic Product Code

We are committed to continually searching for ways to better serve our customers. Ensuring that we always have the selection and quantity of items you want is just one example of that commitment. In an effort to help improve product availability, we are working with our suppliers to introduce electronic product codes, or EPCs, which can be thought of as the next generation of bar codes.

WAL★MART

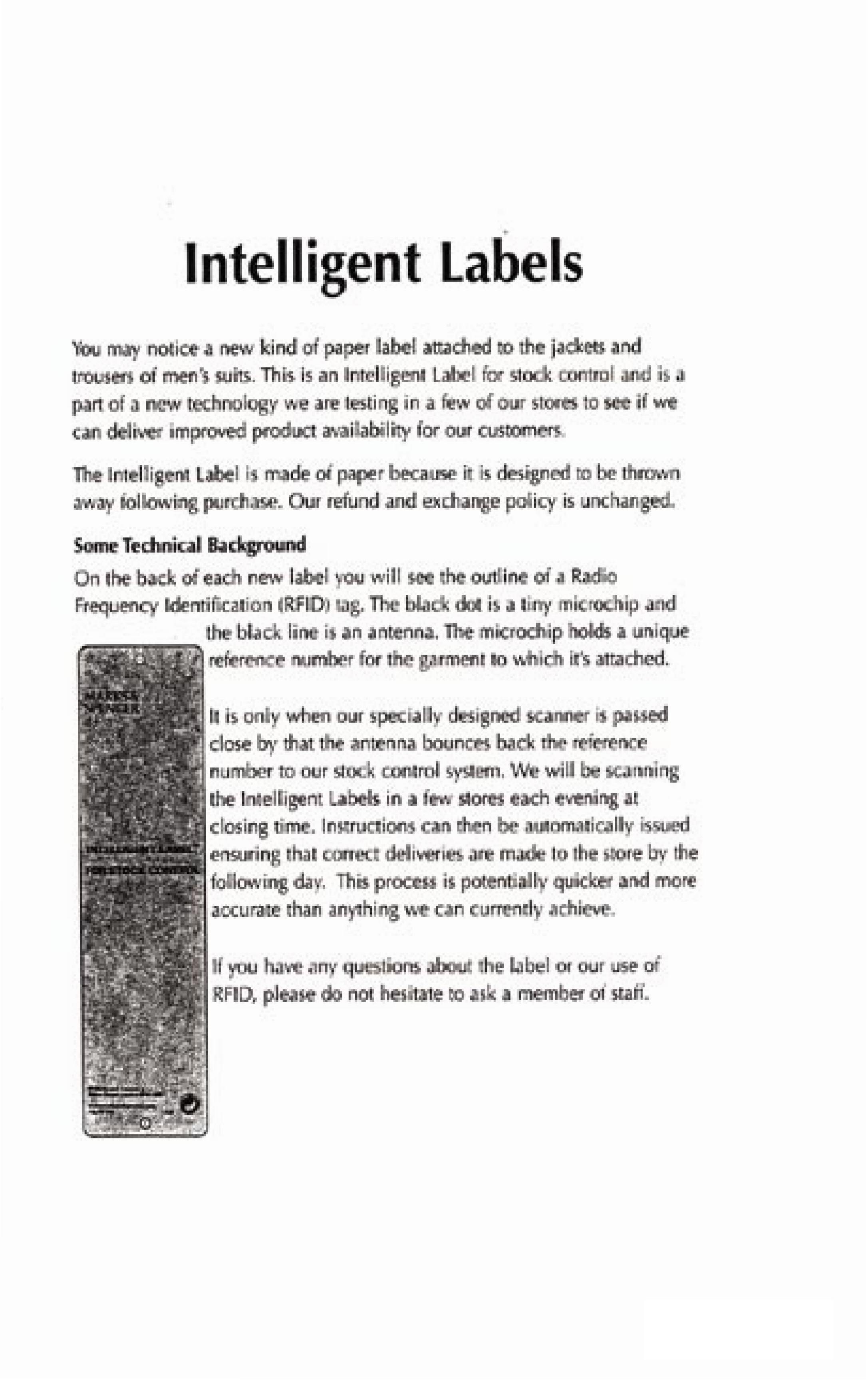
EPCs will strengthen our ability to bring you the items you want, when you want them. By allowing us to locate items from the time they are produced until they arrive at our stores, EPCs will help us manage our inventory more effectively. Our ultimate goal is to continue bringing you quality products at great Every Day Low Prices, as well as providing you with a more enjoyable shopping experience.

Electronic product codes (EPCs) will not be used to collect additional data about our customers or their purchases. EPCs contain only a unique product code and a serial number. This information is stored on a radio frequency identification, or RFID, tag that can only transmit its data when passed near a special reader. That information is then used to ensure there is an ample supply of product available for purchase.

Product cases and pallets will be tagged rather than the individual items, so most customers will only see the benefits of EPCs, not the tags themselves. However, if you are buying a case of products or a large item such as a TV or a computer printer, you may find an RFID tag on the outer packaging of that item. In these instances, the outer packaging will be marked with an EPCglobal symbol (like the one shown on this pamphlet). After purchasing the product, you can choose to keep the tag or discard it.

Customers are our number one priority, and we are committed to ensuring you are informed about this beneficial technology. We hope this information has answered any questions you may have. If you wish to learn more, please visit http://www.epcglobalinc.org/consumer on the Internet or call 1-800-WALMART.

Appendix C: Marks & Spencer "Intelligent Labels" leaflet



Intelligent Labels

You may notice a new kind of paper label attached to the jackets and trousers of men's suits. This is an Intelligent Label for stock control and is a part of a new technology we are testing in a few of our stores to see if we can deliver improved product availability for our customers.

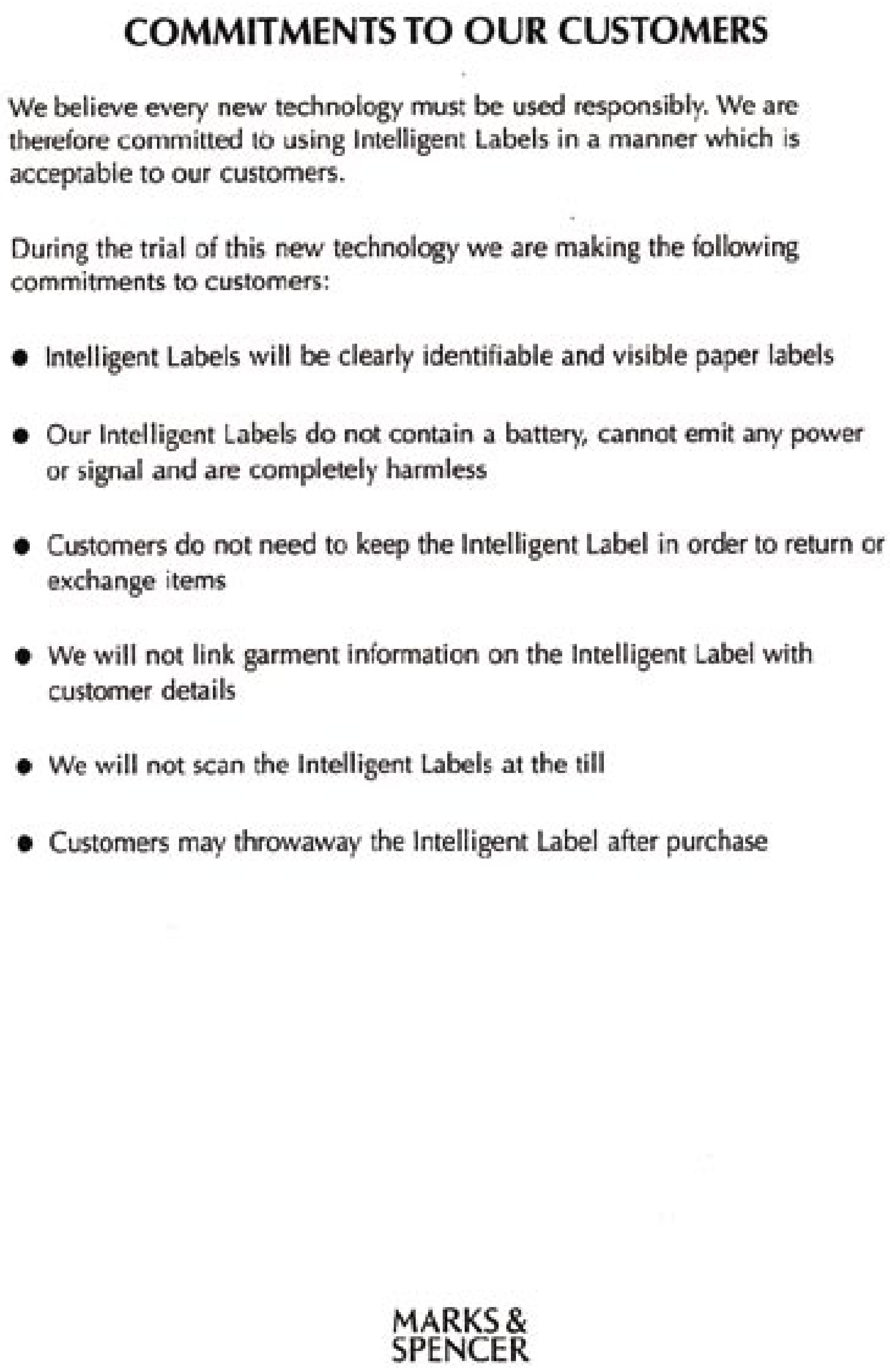
The Intelligent Label is made of paper because it is designed to be thrown away following purchase. Our refund and exchange policy is unchanged.

Some Technical Background

On the back of each new label you will see the outline of a Radio Frequency Identification (RFID) tag. The black dot is a tiny microchip and the black line is an antenna. The microchip holds a unique reference number for the garment to which it's attached.

It is only when our specially designed scanner is passed close by that the antenna bounces back the reference number to our stock control system. We will be scanning the Intelligent Labels in a few stores each evening at closing time. Instructions can then be automatically issued ensuring that correct deliveries are made to the store by the following day. This process is potentially quicker and more accurate than anything we can currently achieve.

If you have any questions about the label or our use of RFID, please do not hesitate to ask a member of staff.



COMMITMENTS TO OUR CUSTOMERS

We believe every new technology must be used responsibly. We are therefore committed to using Intelligent Labels in a manner which is acceptable to our customers.

During the trial of this new technology we are making the following commitments to customers:

- Intelligent Labels will be clearly identifiable and visible paper labels
- Our Intelligent Labels do not contain a battery, cannot emit any power or signal and are completely harmless
- Customers do not need to keep the Intelligent Label in order to return or exchange items
- We will not link garment information on the Intelligent Label with customer details
- We will not scan the Intelligent Labels at the till
- Customers may throwaway the Intelligent Label after purchase

MARKS &
SPENCER

RFID

ftc.gov

1-877-FTC-HELP