Position Statement
on the Use of RFID on Consumer Products

Issued November 14, 2003
Available at www.spychips.com and www.privacyrights.org
==================================

ISSUED BY:

CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) – Principal Author
Privacy Rights Clearinghouse – Principal Author

American Civil Liberties Union (ACLU)   Junkbusters
Electronic Frontier Foundation (EFF)   Meyda Online
Electronic Privacy Information Center (EPIC)   Privacy Activism

ENDORSED BY:

American Council on Consumer Awareness, Inc.   Foundation for Information Policy Research
Association Electronique Libre (AEL)   Simson Garfinkel, Author, Database Nation
Austrian Association for Internet Users   Edward Hasbrouck, Author, The Practical Nomad
Grayson Barber, First Amendment Attorney and   Kriptopolis
   Privacy Advocate   Liberty U.K.
British Columbia Civil Liberties Association   Massachusetts Consumers' Coalition
Canadian Internet Policy and Public Interest Clinic National Association of Consumer Agency
   (CIPPIC)   Associates (NACAA)
Center for Democracy and Technology (CDT)   NoTags.co.uk
Citizens' Council on Health Care   Option Consommateurs
Computer Professionals for Social Responsibility   Privacy International
Consumer Action   Privacy Times
Consumer Assistance Council   Private Citizen, Inc.
Consumer Project on Technology   Privaterra
Deutsche Vereinigung für Datenschutz e.V. (DVD)   Public Interest Advocacy Centre
Electronic Frontier Canada   Quintessenz
Electronic Frontier Finland   Statewatch
Electronic Frontiers Australia   Virginia Rezmierski, Ph.D. Ann Arbor, Michigan
European Digital Rights   World Privacy Forum
FoeBuD e.V., Big Brother Awards Germany
Forum Computer Professionals for Peace and Social
   Responsibility (FIfF)

CONTENTS:

INTRODUCTION

Radio Frequency Identification (RFID) is an item-tagging technology with profound societal implications. Used improperly, RFID has the potential to jeopardize consumer privacy, reduce or eliminate purchasing anonymity, and threaten civil liberties.

As organizations and individuals committed to the protection of privacy and civil liberties, we have come together to issue this statement on the deployment of RFID in the consumer environment. In the following pages, we describe the technology and its uses, define the risks, and discuss potential public policy approaches to mitigate the problems we raise.

RFID tags are tiny computer chips connected to miniature antennae that can be affixed to physical objects. In the most commonly touted applications of RFID, the microchip contains an Electronic Product Code (EPC) with sufficient capacity to provide unique identifiers for all items produced worldwide. When an RFID reader emits a radio signal, tags in the vicinity respond by transmitting their stored data to the reader. With passive (battery-less) RFID tags, read-range can vary from less than an inch to 20-30 feet, while active (self-powered) tags can have a much longer read range. Typically, the data is sent to a distributed computing system involved in, perhaps, supply chain management or inventory control.

THREATS TO PRIVACY AND CIVIL LIBERTIES

While there are beneficial uses of RFID, some attributes of the technology could be deployed in ways that threaten privacy and civil liberties:

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

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

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

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

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

FRAMEWORK OF RFID RIGHTS AND RESPONSIBILITIES

This framework respects businesses' interest in tracking products in the supply chain, but emphasizes individuals' rights to not be tracked within stores and after products are purchased. To mitigate the potential harmful consequences of RFID to individuals and to society, we recommend a three-part framework. First, RFID must undergo a formal technology assessment, and RFID tags should not be affixed to individual consumer products until such assessment takes place. Second, RFID implementation must be guided by Principles of Fair Information Practice. Third, certain uses of RFID should be flatly prohibited.

Technology assessment. RFID must be subject to a formal technology assessment process, sponsored by a neutral entity, perhaps similar to the model established by the now defunct Congressional Office of Technology Assessment. The process must be multi-disciplinary, involving all stakeholders, including consumers.

Principles of Fair Information Practice. RFID technology and its implementation must be guided by strong principles of fair information practices (FIPs). The eight-part Privacy Guidelines of the Organisation for Economic Co-operation and Development (OECD) provides a useful model (www.oecd.org). We agree that the following minimum guidelines, based in part on these principles, must be adhered to while the larger assessment of RFID's societal implications takes place:

- **Openness, or transparency.** RFID users must make public their policies and practices involving the use and maintenance of RFID systems, and there should be no secret databases. Individuals have a right to know when products or items in the retail environment contain RFID tags or readers. They also have the right to know the technical specifications of those devices. Labeling must be clearly displayed and easily understood. Any tag reading that occurs in the retail environment must be transparent to all parties. There should be no tag-reading in secret.

- **Purpose specification.** RFID users must give notice of the purposes for which tags and readers are used.

- **Collection limitation.** The collection of information should be limited to that which is necessary for the purpose at hand.

- **Accountability.** RFID users are responsible for implementation of this technology and the associated data. RFID users should be legally responsible for complying with the principles. An accountability mechanism must be established. There must be entities in both industry and government to whom individuals can complain when these provisions have been violated

- **Security Safeguards.** There must be security and integrity in transmission, databases, and system access. These should be verified by outside, third-party, publicly disclosed assessment.

RFID PRACTICES THAT SHOULD BE FLATLY PROHIBITED

- Merchants must be prohibited from forcing or coercing customers into accepting live or dormant RFID tags in the products they buy.

- There should be no prohibition on individuals to detect RFID tags and readers and disable tags on items in their possession.

- RFID must not be used to track individuals absent informed and written consent of the data subject. Human tracking is inappropriate, either directly or indirectly, through clothing, consumer goods, or other items.

- RFID should never be employed in a fashion to eliminate or reduce anonymity. For instance, RFID should not be incorporated into currency.

ACCEPTABLE USES OF RFID

We have identified several examples of "acceptable" uses of RFID in which consumer-citizens are not subjected to "live" RFID tags and their attendant risks.

- **Tracking of pharmaceuticals** from the point of manufacture to the point of dispensing. RFID tags could help insure that these critical goods are not counterfeit, that they are handled properly, and that they are dispensed appropriately. RFID tags contained on or in the pharmaceutical containers should be physically removed or permanently disabled before being sold to consumers.

- **Tracking of manufactured goods** from the point of manufacture to the location where they will be shelved for sale. RFID tags could help insure that products are not lost or stolen as they move through the supply chain. The tags could also assure the goods are handled appropriately. Tags should be confined to the outside of product packaging (not embedded in the packaging) and be permanently destroyed before consumers interact with them in the store.

- **Detection of items containing toxic substances** when they are delivered to the landfill. For example, when a personal computer is brought to the landfill, a short-range RFID tag could communicate toxic content to a reader at the landfill. It is important to underscore that uses such as the landfill example do not require -- and should not entail -- item-level unique identifiers. The RFID tag would, rather, emit a generic recycling or waste disposal message.

CONCLUSIONS

We are requesting manufacturers and retailers to agree to a voluntary moratorium on the item-level RFID tagging of consumer items until a formal technology assessment process involving all stakeholders, including consumers, can take place. Further, the development of this technology must be guided by a strong set of Principles of Fair Information Practice, ensuring that meaningful consumer control is built into the implementation of RFID. Finally, some uses of RFID technology are inappropriate in a free society, and should be flatly prohibited. Society should not wait for a crisis involving RFID before exerting oversight.

Although not examined in this position paper, we must also grapple with the civil liberties implications of governmental adoption of RFID. The Department of Defense has issued an RFID mandate to its suppliers, schools and libraries in the have begun implementing RFID, the EU and the Japanese government have considered the use of RFID in currency, and British law enforcement has expressed an interest in using RFID as an investigative tool. As an open democratic society, we must adopt a strong policy framework based on Principles of Fair Information Practice to guide governmental implementation of RFID.

Limitations of RFID Technology : Myths Debunked

The following technological limitations have been proposed as reasons why consumers should not be concerned about RFID deployment at this time. We address each perceived limitation in turn, and explain why in themselves, these limitations cannot be relied upon as adequate consumer protection from the risks outlined above.

1. Read-range distances are not sufficient to allow for consumer surveillance.

RFID tags have varying read ranges depending on their antenna size, transmission frequency, and whether they are passive or active. Some passive RFID tags have read ranges of less than one inch. Other RFID tags can be read at distances of 20 feet or more. Active RFID tags theoretically have very long ranges. Currently, most RFID tags envisioned for consumer products are passive with read ranges of under 5 feet.

Contrary to some assertions, tags with shorter read ranges are not necessarily less effective for tracking human beings or items associated with them. In fact, in some cases a shorter read range can be more powerful. For example, if there were an interest in tracking individuals through their shoes as they come within range of a floor reader, a two-inch read range would be preferable to a two-foot read range. Such a short range would help minimize interference with other tags in the vicinity, and help assure the capture of only the pertinent tag positioned directly on the reader.

2. Reader devices not prevalent enough to enable seamless human tracking.

The developers of RFID technology envision a world where RFID readers form a "pervasive global network" It does not take a ubiquitous reader network to track objects or the people associated with them. For example, automobiles traveling up and down Interstate 95 can be tracked without placing RFID readers every few feet. They need only be positioned at the entrance and exit ramps. Similarly, to track an individual's whereabouts in a given town, it is not necessary to position a reader device every ten feet in that town, as long as readers are present at strategic locations such as building entrances.

3. Limited information contained on tags.

Some RFID proponents defend the technology by pointing out that the tags associated with most consumer products will contain only a serial number. However, the number can actually be used as a reference number that corresponds to information contained on one or more Internet-connected databases. This means that the data associated with that number is theoretically unlimited, and can be augmented as new information is collected.

For example, when a consumer purchases a product with an EPC-compliant RFID tag, information about the consumer who purchased it could be added to the database automatically. Additional information could be logged in the file as the consumer goes about her business: "Entered the Atlanta courthouse at 12:32 PM," "At Mobil Gas Station at 2:14 PM," etc. Such data could be accessed by anyone with access to such a database, whether authorized or not.

4. Passive tags cannot be tracked by satellite.

The passive RFID tags envisioned for most consumer products do not have their own power, meaning they must be activated and queried by nearby reader devices. Thus, by themselves, passive tags do not have the ability to communicate via satellites.

However, the information contained on passive RFID tags could be picked up by ambient reader devices which in turn transmit their presence and location to satellites. Such technology has already been used to track the real-time location of products being shipped on moving vehicles through the North American supply chain.

In addition, active RFID tags with their own power source can be enabled with direct satellite transmitting capability. At the present time such tags are far too expensive to be used on most consumer products, but this use is not inconceivable as technology advances and prices fall.

5. High cost of tags make them prohibitive for wide-scale deployment.

RFID developers point to the "high cost" of RFID tags as a way to assuage consumer fears about the power of such tags. However, as technology improves and prices fall, we predict that more and more consumer products will carry tags and that those tags will become smaller and more sophisticated. We predict that the trend will follow the trends of other technical products like computers and calculators.

A Critique of Proposed Industry Solutions

The RFID industry has suggested a variety of solutions to address the dangers posed by RFID tagging of consumer products. Among them are killing the tags at point of sale, the use of "blocker tags," and the "closed system." We examine each strategy in turn.

KILLING TAGS AT POINT OF SALE

Some have proposed that the RFID tag problem could be solved by killing the tags at the point of sale, rendering them inoperable. There are several reasons why we do not believe this approach alone and without other protections will adequately protect consumer privacy:

Killing tags after purchase does not address in-store tracking of consumers.

To date, nearly all consumer privacy invasion associated with RFID tagging of consumer products has occurred within the retail environment, long before consumers reached the checkout counter where chips could be killed. Examples include:

- Close-up photographs were taken of consumers as they picked up RFID-tagged packages of Gillette razor products from store shelves equipped with Auto-ID Center "smart shelf" technology.[1]

- A video camera trained on a Wal-Mart cosmetics shelf in Oklahoma enabled distant Procter and Gamble executives to observe unknowing customers as they interacted with RFID-tagged lipsticks.[2]

- Plans are underway to tag books and magazines with RFID devices to allow detailed in-store observation of people browsing reading materials[3]. This potential was demonstrated recently at the Tokyo International Book Fair 2003. According to Japan's *Nikkei Electronic News*, "By placing tag readers on the shelves of bookstores, the new system allows booksellers to gain information such as the range of books a shopper has browsed, how many times a particular title was picked up and even the length of time spent flipping through each book."

We recognize the need for stores to control shoplifting and make general assessments to enhance operations. However, monitoring and recording the detailed behaviors of consumers without their consent, even if only within the store, violates Principles of Fair Information Practice.

Tags can appear to be "killed" when they are really "asleep" and can be reactivated

Some RFID tags have a "dormant" or "sleep" state that could be set, making it appear to the average consumer that the tag had been killed. It would be possible for retailers and others to claim to have killed a tag when in reality they had simply rendered it dormant. It would be possible to later reactivate and read such a "dormant" tag.

---

[1]   Alorie Gilbert, "Cutting edge 'smart shelf' test ends." CNET News, August 22, 2003.
    Available online at http://news.com.com/2100-1008_3-5067253.html

[2]
  Howard Wolinsky, "P&G, Wal-Mart store did secret test of RFID." The Chicago Sun Times, November 10, 2003.
    Available online at http://www.suntimes.com/output/lifestyles/cst-nws-spy09.html

[3]
  Winston Chai, "Tags track Japanese shoppers." CNET News, May 8, 2003.
    Available online at http://news.zdnet.co.uk/business/0,39020645,2134438,00.htm

The tag killing option could be easily halted by government directive.

It would take very little for a security threat or a change in governmental policies to remove the kill-tag option. If RFID tags are allowed to become ubiquitous in consumer products, removing the kill option could enable the instant creation of a surveillance society.

Retailers might offer incentives or disincentives to consumers to encourage them to leave tags active.

Consumers wishing to kill tags could be required to perform additional steps or undergo burdensome procedures, such as waiting in line for a "killer kiosk"[4] and then being required to kill the tags themselves. Consumers who choose to kill the tags might not enjoy the same discounts or benefits as other consumers, or might not be allowed the same return policies. In many areas of privacy law, this retailer incentive is recognized, and there are legislative prohibitions against inducing the consumer to waive their privacy rights.[5]

The creation of two classes of consumers.

If killing tags requires conscious effort on the part of consumers, many will fail to do so out of fear, ignorance, or lack of time. Many will choose *not* to kill the tags if doing so is inconvenient. (The current "killer kiosk" requires loading one item at a time, a lengthy and time consuming process.) This would create two classes of consumers: those who "care enough" to kill the RFID tags in their products and those who don't. Being a member of either class could have negative ramifications.

BLOCKER TAGS

RFID blocker tags are electronic devices that should theoretically disrupt the transmission of all or select information contained on RFID tags. The proposed blocker tag might be embedded in a shopping bag, purse, or watch that is carried or worn near tags with information consumers want blocked.[6]

Blocker tags are still theoretical.

According to our understanding, the blocker tag does not yet exist. Until a blocker tag is built and tested, there is no way to know how effective it will be and whether it can be technically defeated.

Encourages the widespread deployment of RFID tags.

The blocker tag might encourage the proliferation of RFID devices by giving consumers a false sense of security. While the proposed invention is an ingenious idea, it's one that could be banned or be underutilized if consumers become complacent. It's also possible that such an electronic device could be technically defeated either purposefully or because it stops functioning naturally.

The blocker tag could be banned by government directive or store policy.

Consumers could lose the right to use blocker tag devices if the government deems that knowing what people are wearing or carrying is necessary for national security. They might disallow the devices altogether or name selective spaces in which blocker tags would be disallowed. It is not inconceivable to imagine a ban on such devices in airports or public buildings, for example.

---

[4]
  NCR prototype kiosk kills RFID tags." RFID Journal, September 25, 2003.
     Available online at http://www.rfidjournal.com/article/articleview/585/1/1/
[5]   See e.g., California SB 27, codified at 1798.84 (a).
[6]
  RFID blocker tags developed." Silicon.com, August 28, 2003.
     Available online at http://www.silicon.com/software/applications/0,39024653,10005771,00.htm

Retail stores might ban blocker tags if they believe the tags might be used to circumvent security measures or if they believe knowing details about consumers is valuable in their marketing efforts.

Once RFID tags and readers are ubiquitous in the environment, a full or partial ban on a privacy device like the blocker tag would leave consumers exposed and vulnerable to privacy invasion.

Adds a burden to consumers

A blocker tag shifts the burden of protecting privacy away from the manufacturers and retailers and places it on the shoulders of consumers. In addition, busy consumers might forget to carry blocker devices or forget to implement them, especially if additional steps are required to make them effective.

Fails to protect consumers once products are separated from the blocker tag.

Blocker tags theoretically work only when they are close to the items they are designed to "conceal" from RFID reader devices. Once items are out of the range of the blocking device, consumers would be exposed and vulnerable to privacy invasion. For example, a consumer might buy a sweater and feel that the information on the embedded RFID tag is unexposed because she is carrying it home in a bag impregnated with a blocker device. However, once she removes that sweater from the bag and wears it in range of a reader device, information from that tag could be gleaned.

The creation of two classes of consumers.

Like the kill tag feature, blocker tags will also likely create two classes of consumers, those who block tags and those who do not.

CLOSED SYSTEM

Industry proponents argue that when RFID applications are confined to closed systems, the data is only accessible to those within the system and those with a government mandate (perhaps via legislation such as the Communications Access to Law Enforcement Act (CALEA)). Therefore they argue, society-wide profiling and tracking are not likely. An example of a current closed application is RFID in libraries. *The Grapes of Wrath* in Library X has a different code than the same book in Library Y.

Whereas today RFID applications are confined to closed systems, there will be great incentives to standardize product level tagging. Publishers, for example, may someday ship books to libraries and bookstores with writable tags. Each copy of *The Grapes of Wrath* will contain a portion of its EPC code that is the same as every other copy. The library will be able to customize the remainder of the code to suit its own inventory control purposes.

Even if closed systems remain closed, their lack of transparency makes them troubling from a privacy perspective. Because details about closed systems might not be readily available, consumers could have difficulty obtaining the information necessary to assess privacy risks and protect themselves.

CONCLUSION

We appreciate that industry proponents are making an effort to address consumer privacy and civil liberties concerns associated with RFID technology. However, while we believe the proposed solutions are offered in the proper spirit, they provide inadequate protection. Until appropriate solutions are developed and agreed upon, we believe it is improper to subject consumers to the dangers of RFID technology through item-level consumer product tagging.

SIGNERS

Katherine Albrecht, Director, CASPIAN
Liz McIntyre, Director of Communications, CASPIAN
       www.spychips.com, www.nocards.org
       Media Inquiries: (877) 287-5854, kma@nocards.org
Beth Givens, Director, Privacy Rights Clearinghouse
       www.privacyrights.org
       Media Inquiries: (619) 298-3396, bgivens@privacyrights.org
Lee Tien, Senior Staff Attorney, Electronic Frontier Foundation
       www.eff.org
       Media Inquiries: (415) 436-9333 x 102, tien@eff.org
Jason Catlett, President and Founder, Junkbusters Corp.
       www.junkbusters.com
       Media Inquiries: (908) 512 4608, catlett@junkbusters.org
Deborah Pierce, Executive Director, PrivacyActivism
       www.privacyactivism.org
       Media Inquiries: (415) 225-1730
Barry Steinhardt, Director of the Technology and Liberty Program, American Civil Liberties Union (ACLU)
       www.aclu.org
Kenneth J. Benner, President, American Council on Consumer Awareness, Inc.
       accaus@aol.com
Alexandre Dulaunoy, President, Association Electronique Libre (AEL)
       www.ael.be
Peter Kuhm, Director, Austrian Association for Internet Users
       www.vibe.at
Grayson Barber, First Amendment Attorney and Privacy Advocate
       www.graysonbarber.com
Murray Mollard, Executive Director, British Columbia Civil Liberties Association
       www.bccla.org
Philippa Lawson, Executive Director, Canadian Internet Policy and Public Interest Clinic (CIPPIC)
       www.cippic.ca
Paula Bruening, Staff Counsel, Center for Democracy and Technology
       www.cdt.org
Twila Brase, RN, President, Citizens' Council on Health Care
       www.cchconline.org
Susan Evoy, Managing Director, Computer Professionals for Social Responsibility
       www.cpsr.org
Ken McEldowney, Executive Director, Consumer Action
       www.consumer-action.org
Paul Schrader, Executive Director, Consumer Assistance Council
       www.consumercouncil.com
James Love, Director, Consumer Project on Technology
       www.cptech.org
Dr. Thilo Weichert, President, Deutsche Vereinigung für Datenschutz e.V. (DVD)
       www.aktiv.org/DVD/
Richard S. Rosenberg, Vice-president, Electronic Frontier Canada
       www.efc.ca
Ville Oksanen, Vice Chairman, Electronic Frontier Finland
       www.effi.org
Irene Graham, Executive Director, Electronic Frontiers Australia
       www.efa.org.au
Chris Hoofnagle, Associate Director, Electronic Privacy Information Center (EPIC)
       www.epic.org
Maurice Wessling, President, European Digital Rights

www.edri.org
Rena Tangens & padeluun, FoeBuD e.V., Big Brother Awards Germany
www.foebud.org, www.bigbrotherawards.de
Hans-Joerg Kreowski, Chair, Forum Computer Professionals for Peace and Social Responsibility (FIfF)
http://iug.uni-paderborn.de/fiff
Ian Brown, Director, Foundation for Information Policy Research
www.fipr.org
Simson Garfinkel, Author, Database Nation
Edward Hasbrouck, Author, The Practical Nomad, travel writer and consumer advocate
www.hasbrouck.org
Jose Manuel Gomez, Editor, KRIPTOPOLIS
www.kriptopolis.com
Caoilfhionn Gallagher , Senior Researcher, Liberty U.K.
www.liberty-human-rights.org.uk
Paul J. Schlaver, Chair, Massachusetts Consumers' Coalition
www.massconsumers.org
Jonathan D. Abolins, Author, "Meyda Online: Info Security, Privacy, and Liberties Studies"
www.meydaonline.com
Kathleen Thuner, President, National Association of Consumer Agency Associates (NACAA)
www.nacaanet.org
Chris McDermott, Founder and Director, NoTags.co.uk
www.NoTags.co.uk
Jacques St Amant, Privacy Analyst, Option Consommateurs
www.option-consommateurs.org
Simon Davies, Director, Privacy International
www.privacyinternational.org
Evan Hendricks, Editor, Privacy Times
www.privacytimes.com
Robert Bulmash, President & Founder, Private Citizen, Inc.
www.privatecitizen.com
Robert Guerra, Managing Director, Privaterra
www.privaterra.org
John Lawford, Research Analyst, Public Interest Advocacy Centre
www.piac.ca
Rene Pfeiffer, Board Member, Quintessenz
www.quintessenz.org
Tony Bunyan, Director, Statewatch
www.statewatch.org
Virginia Rezmierski, Ph.D., Ann Arbor, Michigan
Pam Dixon, Executive Director, World Privacy Forum
www.worldprivacyforum.org