Position Statement on the Use of RFID on Consumer Products

November 14, 2003
available at http://www.spychips.org/ and www.privacyrights.org

Issued by:

Consumers Against Supermarket Privacy Invasion and numbering (CASPIAN)
Privacy Rights Clearinghouse
American Civil Liberties Union (ACLU)
Electronic Frontier Foundation (EFF)
Electronic Privacy Information Center (EPIC)
Junkbusters
Meyda Online
PrivacyActivism

Endorsed By:

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

- FoeBuD e.V., Big Brother Awards Germany
- Forum Computer Professionals for Peace and Social Responsibility (FIfF)
- Foundation for Information Policy Research

Contents:

I. Introduction

Radio Frequency Identification (RFID) is an item-tagging technology with profound RFID has the potential to jeopardize consumer privacy, reduce or eliminate purcha liberties.

As organizations and individuals committed to the protection of privacy and civil lib this statement on the deployment of RFID in the consumer environment. In the foll technology and its uses, define the risks, and discuss potential public policy appro

RFID tags are tiny computer chips connected to miniature antennae that can be at commonly touted applications of RFID, the microchip contains an Electronic Produc provide unique identifiers for all items produced worldwide. When an RFID reader e respond by transmitting their stored data to the reader. With passive (battery-less) than an inch to 20-30 feet, while active (self-powered) tags can have a much longe to a distributed computing system involved in, perhaps, supply chain management

II. Threats to Privacy and Civil Liberties

While there are beneficial uses of RFID, some attributes of the technology could b and civil liberties:

- Hidden placement of tags. RFID tags can be embedded into/onto objects and the individual who obtains those items. As radio waves travel easily and silentl materials, it is possible to read RFID tags sewn into clothing or affixed to objec suitcases, and more.

- Unique identifiers for all objects worldwide. The Electronic Product Code poten have its own unique ID. The use of unique ID numbers could lead to the creati which every physical object is identified and linked to its purchaser or owner at
- Massive data aggregation. RFID deployment requires the creation of massive These records could be linked with personal identifying data, especially as con

expand.

- Hidden readers. Tags can be read from a distance, not restricted to line of sig invisibly into nearly any environment where human beings or items congregate experimentally embedded into floor tiles, woven into carpeting and floor mats, incorporated into retail shelving and counters, making it virtually impossible for was being "scanned."

- Individual tracking and profiling. If personal identity were linked with unique RF profiled and tracked without their knowledge or consent. For example, a tag er facto identifier for the person wearing it. Even if item-level information remains carry could associate them with, for example, particular events like political ralli

III. Framework of RFID Rights and Responsibilities

This framework respects businesses' interest in tracking products in the supply cha not be tracked within stores and after products are purchased. To mitigate the pot individuals and to society, we recommend a three-part framework. First, RFID must assessment, and RFID tags should not be affixed to individual consumer products Second, RFID implementation must be guided by Principles of Fair Information Pra be flatly prohibited.

Technology assessment. RFID must be subject to a formal technology assessmen perhaps similar to the model established by the now defunct Congressional Office must be multi-disciplinary, involving all stakeholders, including consumers.

Principles of Fair Information Practice. RFID technology and its implementation mu information practices (FIPs). The eight-part Privacy Guidelines of the Organisation Development (OECD) provides a useful model (http://www.oecd.org/). We agree th based in part on these principles, must be adhered to while the larger assessment place:

- Openness, or transparency. RFID users must make public their policies and pr maintenance of RFID systems, and there should be no secret databases. Indiv products or items in the retail environment contain RFID tags or readers. They specifications of those devices. Labeling must be clearly displayed and easily in the retail environment must be transparent to all parties. There should be nc

- Purpose specification. RFID users must give notice of the purposes for which t

- Collection limitation. The collection of information should be limited to that whic

- Accountability. RFID users are responsible for implementation of this technolog should be legally responsible for complying with the principles. An accountabili There must be entities in both industry and government to whom individuals ca been violated.

- Security Safeguards. There must be security and integrity in transmission, data should be verified by outside, third-party, publicly disclosed assessment.

IV. RFID Practices that Should be Flatly Prohibited:

- Merchants must be prohibited from forcing or coercing customers into acceptin products they buy.

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

- RFID must not be used to track individuals absent informed and written consen inappropriate, either directly or indirectly, through clothing, consumer goods, or

- RFID should never be employed in a fashion to eliminate or reduce anonymity.

incorporated into currency.

V. Acceptable Uses of RFID

We have identified several examples of "acceptable" uses of RFID in which consur RFID tags and their attendant risks.

- Tracking of pharmaceuticals from the point of manufacture to the point of disp these critical goods are not counterfeit, that they are handled properly, and th RFID tags contained on or in the pharmaceutical containers should be physica before being sold to consumers.

- Tracking of manufactured goods from the point of manufacture to the location tags could help insure that products are not lost or stolen as they move throug assure the goods are handled appropriately. Tags should be confined to the embedded in the packaging) and be permanently destroyed before consumers

- Detection of items containing toxic substances when they are delivered to the computer is brought to the landfill, a short-range RFID tag could communicate is important to underscore that uses such as the landfill example do not require unique identifiers. The RFID tag would, rather, emit a generic recycling or wast

VI. Conclusions

We are requesting manufacturers and retailers to agree to a voluntary moratorium consumer items until a formal technology assessment process involving all stakeho place. Further, the development of this technology must be guided by a strong set ensuring that meaningful consumer control is built into the implementation of RFID. are inappropriate in a free society, and should be flatly prohibited. Society should r exerting oversight.

Although not examined in this position paper, we must also grapple with the civil lib adoption of RFID. The Department of Defense has issued an RFID mandate to its have begun implementing RFID, the EU and the Japanese government have cons British law enforcement has expressed an interest in using RFID as an investigativ we must adopt a strong policy framework based on Principles of Fair Information P implementation of RFID.

VII. RFID Position Paper Attachment 1
November 14, 2003

Limitations of RFID Technology : Myths Debunked

The following technological limitations have been proposed as reasons why consu RFID deployment at this time. We address each perceived limitation in turn, and ex limitations cannot be relied upon as adequate consumer protection from the risks

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

RFID tags have varying read ranges depending on their antenna size, transmissio passive or active. Some passive RFID tags have read ranges of less than one inch distances of 20 feet or more. Active RFID tags theoretically have very long ranges. consumer products are passive with read ranges of under 5 feet.

Contrary to some assertions, tags with shorter read ranges are not necessarily less items associated with them. In fact, in some cases a shorter read range can be mo an interest in tracking individuals through their shoes as they come within range of would be preferable to a two-foot read range. Such a short range would help minir vicinity, and help assure the capture of only the pertinent tag positioned directly or

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

The developers of RFID technology envision a world where RFID readers form a "p a ubiquitous reader network to track objects or the people associated with them. F

and down Interstate 95 can be tracked without placing RFID readers every few fee entrance and exit ramps. Similarly, to track an individual's whereabouts in a given t reader device every ten feet in that town, as long as readers are present at strateg

3. Limited information contained on tags.

Some RFID proponents defend the technology by pointing out that the tags associ contain only a serial number. However, the number can actually be used as a refe information contained on one or more Internet-connected databases. This means number is theoretically unlimited, and can be augmented as new information is col

For example, when a consumer purchases a product with an EPC-compliant RFID purchased it could be added to the database automatically. Additional information consumer goes about her business: "Entered the Atlanta courthouse at 12:32 PM, Such data could be accessed by anyone with access to such a database, whethe

4. Passive tags cannot be tracked by satellite. The passive RFID tags envisioned f their own power, meaning they must be activated and queried by nearby reader de tags do not have the ability to communicate via satellites.

However, the information contained on passive RFID tags could be picked up by a transmit their presence and location to satellites. Such technology has already bee products being shipped on moving vehicles through the North American supply ch

In addition, active RFID tags with their own power source can be enabled with dire present time such tags are far too expensive to be used on most consumer produc 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 consu However, as technology improves and prices fall, we predict that more and more co those tags will become smaller and more sophisticated. We predict that the trend w products like computers and calculators.

VIII. RFID Position Paper Attachment 2
November 14, 2003

Critque of Proposed Industry Solutions

The RFID industry has suggested a variety of solutions to address the dangers po products. Among them are killing the tags at point of sale, the use of "blocker tags 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 inoperable. There are several reasons why we do not believe this approach alone 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 cons retail environment, long before consumers reached the checkout counter where ch

- Close-up photographs were taken of consumers as they picked up RFID-tagge 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 di observe unknowing customers as they interacted with RFID-tagged lipsticks.[2]
- Plans are underway to tag books and magazines with RFID devices to allow d browsing reading materials.[3]

This potential was demonstrated recently at the Tokyo International Book Fair 200

News, “By placing tag readers on the shelves of bookstores, the new system allow the range of books a shopper has browsed, how many times a particular title was spent flipping through each book.”

We recognize the need for stores to control shoplifting and make general assessm monitoring and recording the detailed behaviors of consumers without their consen Principles of Fair Information Practice.

Tags can appear to be “killed” when they are really "asleep" and can be reactivate

Some RFID tags have a “dormant” or “sleep” state that could be set, making it app tag had been killed. It would be possible for retailers and others to claim to have ki rendered it dormant. It would be possible to later reactivate and read such a “dorm

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 are allowed to become ubiquitous in consumer products, removing the kill option c surveillance society.

Retailers might offer incentives or disincentives to consumers to encourage them t

Consumers wishing to kill tags could be required to perform additional steps or unc waiting in line for a "killer kiosk"[4] and then being required to kill the tags themselv tags might not enjoy the same discounts or benefits as other consumers, or might In many areas of privacy law, this retailer incentive is recognized, and there are leg 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 d time. Many will choose not to kill the tags if doing so is inconvenient. (The current “ time, a lengthy and time consuming process.) This would create two classes of cor the RFID tags in their products and those who don't. Being a member of either cla

Blocker Tags

RFID blocker tags are electronic devices that should theoretically disrupt the transm contained on RFID tags. The proposed blocker tag might be embedded in a shopp 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 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 consu proposed invention is an ingenious idea, it’s one that could be banned or be unde complacent. It’s also possible that such an electronic device could be technically d 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 deem or carrying is necessary for national security. They might disallow the devices altog blocker tags would be disallowed. It is not inconceivable to imagine a ban on such example.

Retail stores might ban blocker tags if they believe the tags might be used to circu 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 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 shoulders of consumers. In addition, busy consumers might forget to carry blocker 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 desig devices. Once items are out of the range of the blocking device, consumers would invasion. For example, a consumer might buy a sweater and feel that the informati unexposed because she is carrying it home in a bag impregnated with a blocker d sweater from the bag and wears it in range of a reader device, information from th

The creation of two classes of consumers.

Like the kill tag feature, blocker tags will also likely create two classes of consumer do not.

Closed System

Industry proponents argue that when RFID applications are confined to closed sys those within the system and those with a government mandate (perhaps via legisla Access to Law Enforcement Act (CALEA)). Therefore they argue, society-wide prof example of a current closed application is RFID in libraries. The Grapes of Wrath ir same book in Library Y.

Whereas today RFID applications are confined to closed systems, there will be gre tagging. Publishers, for example, may someday ship books to libraries and booksto Grapes of Wrath will contain a portion of its EPC code that is the same as every ot 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 troub details about closed systems might not be readily available, consumers could have necessary to assess privacy risks and protect themselves.

Conclusion

We appreciate that industry proponents are making an effort to address consumer associated with RFID technology. However, while we believe the proposed solution provide inadequate protection. Until appropriate solutions are developed and agree subject consumers to the dangers of RFID technology through item-level consume

IX. Signers

Katherine Albrecht, Director, CASPIAN, http://www.spychips.org/
Media Inquiries: (877) 287-5854, kma@nocards.org

Liz McIntyre, Director of Communications, CASPIAN, http://www.nocards.org/
Media Inquiries: (877) 287-5854, liz@nocards.org

Beth Givens, Director, Privacy Rights Clearinghouse,
http://www.privacyrights.org/../../../DOCUME~1/JBEEBE~1/LOCALS~1/Temp/FrontI
Media Inquiries: (619) 298-3396, bgivens@privacyrights.org

Lee Tien, Senior Staff Attorney, Electronic Frontier Foundation, http://www.eff.org/
Media Inquiries: (415) 436-9333 x 102, tien@eff.org

Jason Catlett, President and Founder, Junkbusters Corp.,
http://www.privacyrights.org/../../../DOCUME~1/JBEEBE~1/LOCALS~1/Temp/FrontI
Media Inquiries: (908) 512 4608, catlett@junkbusters.org

Deborah Pierce, Executive Director, PrivacyActivism, http://www.privacyactivism.org
Media Inquiries: (415) 225-1730

Barry Steinhardt, Director of the Technology and Liberty Program, American Civil L
http://www.privacyrights.org/../../../DOCUME~1/JBEEBE~1/LOCALS~1/Temp/Front

Kenneth J. Benner, President, American Council on Consumer Awareness, Inc., ac

Alexandre Dulaunoy, President, Association Electronique Libre (AEL), http://www.a

Peter Kuhm, Director, Austrian Association for Internet Users, http://www.vibe.at/

Grayson Barber, First Amendment Attorney and Privacy Advocate, http://www.gray

Murray Mollard, Executive Director, British Columbia Civil Liberties Association, http

Philippa Lawson, Executive Director, Canadian Internet Policy and Public Interest C

Paula Bruening, Staff Counsel, Center for Democracy and Technology,
http://www.privacyrights.org/../../../DOCUME~1/JBEEBE~1/LOCALS~1/Temp/Front

Twila Brase, RN, President, Citizens' Council on Health Care, http://www.cchconlin

Susan Evoy, Managing Director, Computer Professionals for Social Responsibility,

Ken McEldowney, Executive Director, Consumer Action,
http://www.privacyrights.org/../../../DOCUME~1/JBEEBE~1/LOCALS~1/Temp/Front

Paul Schrader, Executive Director, Consumer Assistance Council,
http://www.privacyrights.org/../../../DOCUME~1/JBEEBE~1/LOCALS~1/Temp/Front

James Love, Director, Consumer Project on Technology,
http://www.privacyrights.org/../../../DOCUME~1/JBEEBE~1/LOCALS~1/Temp/Front

Dr. Thilo Weichert, President, Deutsche Vereinigung für Datenschutz e.V. (DVD), w

Richard S. Rosenberg, Vice-president, Electronic Frontier Canada, http://www.efc.

Ville Oksanen, Vice Chairman, Electronic Frontier Finland, http://www.effi.org/

Irene Graham, Executive Director, Electronic Frontiers Australia, http://www.efa.org

Chris Hoofnagle, Associate Director, Electronic Privacy Information Center (EPIC),
http://www.privacyrights.org/../../../DOCUME~1/JBEEBE~1/LOCALS~1/Temp/Front

Maurice Wessling, President, European Digital Rights, http://www.edri.org/

Rena Tangens & padeluun, FoeBuD e.V., Big Brother Awards Germany, http://ww
http://www.bigbrotherawards.de/

Hans-Joerg Kreowski, Chair, Forum Computer Professionals for Peace and Social I
http://iug.uni-paderborn.de/fiff

Ian Brown, Director, Foundation for Information Policy Research, http://www.fipr.or

Simson Garfinkel, Author, Database Nation

Edward Hasbrouck, Author, The Practical Nomad, travel writer and consumer advo

Jose Manuel Gomez, Editor, KRIPTOPOLIS, http://www.kriptopolis.com/

Caoilfhionn Gallagher , Senior Researcher, Liberty U.K., http://www.liberty-human-r

Paul J. Schlaver, Chair, Massachusetts Consumers' Coalition, http://www.masscons

Jonathan D. Abolins, Author, "Meyda Online: Info Security, Privacy, and Liberties
http://www.privacyrights.org/../../../DOCUME~1/JBEEBE~1/LOCALS~1/Temp/Front

Kathleen Thuner, President, National Association of Consumer Agency Associates

Chris McDermott, Founder and Director, NoTags.co.uk, http://www.notags.co.uk/

Jacques St Amant, Privacy Analyst, Option Consommateurs, http://www.option-cor

Simon Davies, Director, Privacy International, http://www.privacyinternational.org/

Evan Hendricks, Editor, Privacy Times, http://www.privacyrights.org/../../../DOCUME~1/JBEEBE~1/LOCALS~1/Temp/FrontP

Robert Bulmash, President & Founder, Private Citizen, Inc., http://privatecitizen.co

Robert Guerra, Managing Director, Privaterra, http://www.privaterra.org/

John Lawford, Research Analyst, Public Interest Advocacy Centre, http://www.piac

Rene Pfeiffer, Board Member, Quintessenz, http://www.quintessenz.org/

Tony Bunyan, Director, Statewatch, http://www.statewatch.org/

Virginia Rezmierski, Ph.D., Ann Arbor, Michigan

Pam Dixon, Executive Director, World Privacy Forum, http://www.privacyrights.org/../../../DOCUME~1/JBEEBE~1/LOCALS~1/Temp/FrontP

[1] Alorie Gilbert, “Cutting edge 'smart shelf' test ends.” CNET News, August 22, 2(http://news.com.com/2100-1008_3-5067253.html

[2] Howard Wolinsky, “P&G, Wal-Mart store did secret test of RFID.” The Chicago S online at http://www.suntimes.com/output/lifestyles/cst-nws-spy09.html

[3] Winston Chai, “Tags track Japanese shoppers.” CNET News, May 8, 2003. Ava http://news.zdnet.co.uk/business/0,39020645,2134438,00.html

[4] "NCR prototype kiosk kills RFID tags.” RFID Journal, September 25, 2003. Avai 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 a http://www.silicon.com/software/applications/0,39024653,10005771,00.html