TACD

TRANS ATLANTIC CONSUMER DIALOGUE
DIALOGUE TRANSATLANTIQUE DES CONSOMMATEURS

DOC NO. INTERNET-31-05 DATE ISSUED: APRIL, 2005

RESOLUTION ON RADIO-FREQUENCY IDENTIFICATION (RFID)

Introduction

The Trans Atlantic Consumer Dialogue (TACD) believes action is urgently needed to address the potential risks of radio-frequency identification technology (RFID). While RFID can be used to benefit consumers, it also poses risks that have yet to be fully recognised and addressed.

The Technology

The use of RFID is predicted to increase substantially in the near future. RFID is an identification and tracking technology, likely to form a key cornerstone of ubiquitous computing. It is also often referred to as the most probable successor to barcode technology.

RFID uses tags containing microchips with antennae that can be embedded into things or attached as labels. These chips broadcast a unique number when woken up by a scanner's radio signals. This allows each item to be identified and tracked individually, unlike barcodes, which use generic product codes.

Passive tags can be as small as a grain of sand and have no batteries (so they are powered by a scanner's signal, up to 17 feet or 5m away). Larger (and more expensive) tags have their own power and a greater transmission range. Scanners can be mobile or static – a scanner that can be attached to a mobile phone is already on the market.

To focus on retail, tags were initially used to track batches of goods through the supply chain, from manufacturers' premises to delivery at retail outlets. As the cost of tags has fallen, there is now a move to tag individual items. This holds numerous attractions for retailers, including the possibility of simultaneously scanning the entire contents of shopping carts, as tags (unlike barcodes) do not require a line of sight for goods to be read.

RFID can be used in almost countless ways, to tag individual products, animals and even people. Lobsters, for example, have already been tagged in the Gulf of Maine for conservation reasons, and cattle can be tracked in the food supply chain to increase food safety. People can be injected with tags: some regulars at a nightclub in Barcelona, Spain, have been injected with tags that allow them to enter the club and pay for drinks automatically.

RFID can offer tangible consumer benefits, whether to improve the availability of products in stores or to tag vital hospital equipment (which can then be located quickly in an emergency). It is a technology in transition – how it will continue to be developed and implemented in future remains to be seen.

Risks for Consumers

Nevertheless, the roll-out of RFID does involve significant risks for consumers:

Surveillance and privacy: RFID is likely to play a major role in the development of pervasive computing. But the use of item-level tagging may involve unwanted surveillance, threatening consumers' privacy and dignity. The danger of living with 'chips with everything' is that surveillance is automated on an unprecedented scale.

If consumers are linked with unique tag numbers, they could be profiled and tracked – with or without their consent. Consumers could, for instance, be recognised, monitored and marketed to more efficiently in-store, through the items they carry or wear (such as RFID-chipped credit or loyalty cards). Purchasing anonymity could become a thing of the past, aided by the advent of common tag standards and scanners that could facilitate widespread tag recognition and tracking.

RFID tags can be embedded into objects without consumers realising. For instance, it is possible to read RFID tags that have been sewn into clothing. Scanners also may be developed to be easily disguised (one prediction is that scanners could be embedded in floor tiles and carpeting). As the Article 29 Working Party (2005) has written:

> "THE ABILITY TO SURREPTITIOUSLY COLLECT A VARIETY OF DATA ALL RELATED TO THE SAME PERSON; TRACK INDIVIDUALS AS THEY WALK IN PUBLIC PLACES (AIRPORTS, TRAIN STATIONS, STORES); ENHANCE PROFILES THROUGH THE MONITORING OF CONSUMER BEHAVIOUR IN STORES; READ THE DETAILS OF CLOTHES AND ACCESSORIES WORN AND MEDICINES CARRIED BY CONSUMERS ARE ALL EXAMPLES OF USES OF RFID TECHNOLOGY THAT GIVE RISE TO PRIVACY CONCERNS. THE PROBLEM IS AGGRAVATED BY THE FACT THAT, DUE TO ITS RELATIVE LOW COST, THIS TECHNOLOGY WILL NOT ONLY BE AVAILABLE TO MAJOR ACTORS BUT ALSO TO SMALLER PLAYERS AND INDIVIDUAL CITIZENS."

Security and identity theft: The security of RFID is also a concern. There is the risk of interception, as the cheapest tags do not incorporate sophisticated data encryption functions. In a recent experiment at John Hopkins University (2005), students demonstrated that they could easily defeat the encryption in a popular RFID system used to deter car theft and purchase gasoline.

Currently, governments also are considering embedding RFID in passports and other identity documents but without sufficient security. RFID used in identification documents without adequate security is likely to substantially increase identity theft, as these documents could be remotely scanned and duplicated with relative ease.

While security could be enhanced by the development and use of standards, the standards process has yet to fully engage with consumers' interests and effectively involve consumer representatives.

Consumer discrimination: RFID may contribute to the ever more efficient collection and analysis of huge amounts of data on consumers. This could enable the increasingly accurate identification of the most profitable consumers, who will be offered the best deals, and the increased exclusion of less profitable consumers from markets. RFID could, for instance, facilitate dynamic pricing, so that more desirable consumers receive special in-store offers (perhaps delivered through screens on their shopping carts).

Competition: RFID could be used in ways that restrict consumer choice. Organisations could use RFID in applications that control the use of products or force consumers to use products that are more costly. To give a hypothetical example, a printer could be tagged so

that it only accepts the ink-refills of a certain manufacturer. Similarly, a vehicle manufacturer could design software that, when used in conjunction with RFID technology, ties the use of branded spare parts to their vehicles.

Crime: Fears exist that RFID-tagged items will become easy prey for thieves. As the Article 29 Working Party has written: "For a few years, the mere presence of an RFID tag… will help thieves looking for items worth stealing in cloakrooms or parking garages."

Automated shopping: Proponents of the technology have argued that RFID will make consumers' lives easier. They argue, for example, that RFID will promote a more efficient retail experience as check-out queues will be reduced substantially. But the increased automation unleashed by RFID may alienate some consumers, particularly those who welcome or need a more personalised service, including those who are technologically-challenged.

Health: Some organisations have questioned whether the radiation emitted by RFID will be safe, if RFID is used widely in the future. Even if radiation is currently estimated as being comparatively low, no risk assessment has been carried out yet.

RFID studies show consumer concerns about privacy: At present, consumers know little about the technology but tend to be worried by it. A recent survey of consumers in the UK, France, Germany and the Netherlands found that more than half (55%) of the people surveyed said they were either concerned or very concerned that RFID would allow businesses to track consumers via product purchases (BBC 2005). And 59% said they were worried that RFID would allow data to be used more freely by third parties.

Another recent survey by Artafact LLC and BIGresearch revealed that a majority of consumers who were aware of RFID technologies were "very or somewhat concerned about invasion of privacy issues." 88% of respondents concerned with privacy cited the government as the organization most likely to abuse consumers' personal information, followed by "crooks and bad guys," banks, insurance companies and credit card companies.

Lack of consumer protection, involvement and choice: Consumer interests may become marginalised in the race to adopt RFID. Deliberative structures that would enable consumer involvement in the technology's future are not yet in place. On the ground, RFID may be rolled out without sufficiently addressing consumer concerns.

Consumers' responses to the technology will be crucial to its future – there is a growing awareness that RFID must be used responsibly. In November 2003, a number of civil liberty organisations issued a position statement on the use of RFID in consumer products (Position Statement 2003). More recently, in January 2005, the EU's Article 29 Data Protection Working Party published a working document, which provided guidance on the use of RFID.

Recommendations

TACD therefore resolves that the EU and US governments should:

1. Analyze whether existing data protection and privacy regulations adequately address the privacy risks that the applications of RFID present for consumers in different contexts and sectors; determine the appropriate safeguards; and enact the legislation and regulations necessary to eliminate those risks.

2. Ensure that the implementation of RFID technology complies with existing data protection and privacy legislation (such as the Data Protection Directive and the Directive on Privacy and Electronic Communications in the EU) and privacy

guidelines (such as the OECD's principles of fair information practice). For example, RFID must be used transparently, so that consumers know (and can choose) when RFID is being used; and know who is collecting the data and why. Consumers must also be given the right to access their information. In particular, the EU and US governments should require organisations developing and using RFID to follow the following principles (the first four (a – d) are set out in the International Conference of Data Protection & Privacy Commissioners "Resolution on Radio Frequency Identification Technology", 2003):

a. Before introducing RFID tags linked to personal information or which help build consumer profiles, organisations should first consider alternatives that achieve the same goal without collecting personal information or profiling consumers;

b. If organisations can show that personal data are indispensable, they must be collected in an open and transparent way;

c. Personal data should only be used for the specific purpose for which they were first collected and only retained for as long as is necessary to achieve that purpose;

d. Whenever consumers possess RFID tags, they should be given the option of deleting data and disabling the tags;

e. Any ID-based RFID should be designed to be accessible only with the consent of the person.

3. Finally, at retail-level there should always be the possibility to pay anonymously without using payment-cards, store cards or any other personal data payment system.

4. Vigorously enforce laws and regulations that apply to RFID.

5. Monitor whether RFID is being used in anti-competitive ways, and use anti-competition laws to prevent such abuse.

6. Consult with all RFID stakeholders, including consumer organizations and independent academic researchers, to tap into the range of expertise that could usefully contribute to this debate.

7. Fund ongoing research into the impact of RFID on consumers, particularly those who are disadvantaged (such as those who are disabled and on low incomes), and their perceptions of the technology. Research must be undertaken in a transparent, independent, and scientific way.

8. Require organisations that use RFID to automatically de-activate the tag after the consumer has purchased the product, giving the consumer the option of re-activating the tag where that might be appropriate.

9. Commission independent and scientific research to investigate the safety of RFID and its environmental impact.

Furthermore, TACD resolves that organisations developing and using RFID should:

1. Provide evidence of real consumer benefits from the use of RFID and address its potential risks. If organisations make claims that specific consumer benefits will accrue from using RFID, these promised benefits must be delivered.

2. Build security and privacy protection into the technology and its applications. This would include ensuring that sensitive data are encrypted and that data confidentiality and integrity is maintained (so that, for example, information is protected from unauthorised third-party access). Protection must not be seen as an optional extra but as an integral part of deploying this technology.

3. Explore positive uses of the technology that enhance consumer privacy and decision-making. For example, scanners could alert consumers to opportunities to make choices, access information on products, and offer real-time access to their data.

4. Explore the potential of RFID to extend consumer choice and reject applications that have potentially anti-competitive effects.

USEFUL REFERENCES

Artafact LLC and BIGresearch study: http://www.bigresearch.com/rfid.htm

Article 29 Data Protection Working Party (2005) "Working document on data protection issues related to RFID technology": www.europa.eu.int/comm/privacy

Auto-ID Center/Proctor & Gamble survey (2001): http://cryptome.org/rfid/pk-fh.pdf

BBC (2005) "Consumer concern over RFID tags": http://news.bbc.co.uk/1/hi/technology/4247275.stm

EPIC's RFID Page: http://www.epic.org/privacy/rfid

EPIC's comments to the FTC RFID workshop, June 21, 2004: http://www.epic.org/privacy/rfid/ftc-comts-070904.pdf.

EPIC's Privacy Guidelines for RFID Technology:
http://www.epic.org/privacy/rfid/rfid_gdlnes-070904.pdf (final version, July 9, 2004)

Hearing on "Radio Frequency Identification (RFID) Technology: What the Future Holds for Commerce, Security, and the Consumer" before the Subcommittee on Commerce, Trade, and Consumer Protection, US House of Representatives, July 14, 2004:

- EPIC's testimony:
http://energycommerce.house.gov/108/Hearings/07142004hearing1337/Laurant2152.htm

- ACLU's testimony:
http://energycommerce.house.gov/108/Hearings/07142004hearing1337/Steinhardt2150.htm

International Conference of Data Protection & Privacy Commissioners (2003) "Resolution on Radio-Frequency Identification Technology": http://www.privacyconference2003.org/resolutions/res5.DOC

John Hopkins RFID Research Project (2005): http://rfidanalysis.org

Lace, Susanne (2004) "Calling in the chips? Findings from the first summit exploring the future of RFID technology in retail" National Consumer Council: London:
http://www.ncc.org.uk/technology/calling_in_chips.pdf

OECD (2004) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data:
http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

Position Statement (2003) on the Use of RFID on Consumer Products, November 2003: www.privacyrights.org/ar/RFIDposition.htm