Electronic Privacy Information Center (EPIC)
Washington, DC

Comments submitted in consideration of
the Article 29 Data Protection Working Party
"Working Document on Data Protection Issues related to RFID Technology"

1. INTEREST OF COMMENTATOR

The Electronic Privacy Information Center (EPIC) is a public interest research organization in Washington, DC established in 1994 to focus public attention on emerging civil liberties issues. Each year EPIC publishes *Privacy and Human Rights: An International Survey of Privacy Law and Developments*. The 2004 edition of the *Privacy and Human Rights* report contains an extensive discussion of privacy issues associated with the development of Radio Frequency Identification (RFID).

2. SUMMARY

On January 19, 2005, the Article 29 Working Party released a document entitled "Working Document on data protection issues related to RFID technology" (the "RFID Working Document"). EPIC appreciates the opportunity to submit comments on this document.

The awareness of the risks related to the use of RFID technology has compelled the Article 29 Data Protection Working Party to produce a document that looks into the privacy and other implications of RFID technology for fundamental rights.[1] There are already multiple examples of RFID uses in the private and public sectors. The RFID Working Document makes clear the need to comply with the basic principles set out in the European Community Data Protection Directives,[2] whenever personal data is collected using RFID technology. The RFID Working Document also provides useful guidance for the development of RFID-enabled products.

While EPIC supports many of the views set out in the RFID Working Document, we also welcome the opportunity to raise a few concerns and recommendations.

---

[1] Working Document on Data Protection Issues related to RFID Technology, January 19, 2005 [RFID Working Document] available at: http://europa.eu.int/comm/internal_market/privacy/workingroup/consultations/consultation_en.htm.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281), available at: http://europa.eu.int/eur-lex/en/lif/dat/1995/en_ 395L0046.html and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) Official Journal L 201, 31/07/2002.

EPIC proposes the following recommendations, which are described in more detail in our comments below:

- Review of the introductory paragraph to make clear importance of establishing public trust and confidence in development of RFID applications;
- Thorough assessment of privacy and security issues conducted prior to implementing RFID technology;
- Adoption of a "Four Tier Approach to RFID Policy" in relation to RFID's applications in healthcare sector;
- General prohibition of the RFID implants;
- General prohibition of unencrypted electronic passports in conjunction with thorough assessment of any technology to be used in the travel documents;
- Implementation of strong privacy Guidelines such as EPIC's RFID Privacy Guidelines for businesses deploying RFID technology on individual consumer products;
- Introduction of contact-based chips, or other visualization technologies, against unauthorized read-out of the RFID chips;
- Addressing the problem of a transfer of tagged-goods to third parties and the subsequent problem of their consent;
- Implementation of uniform standards in terms of deactivation of the tag as well as encryption of any personal data stored in the chip's memory;
- Alternation of wording as far as encryption for sensitive data is concerned;
- Implementation of a truly responsive legal framework that seeks to accommodate values of technology and privacy;

3. RECOMMENDATIONS

In the introductory paragraph, the RFID Working Document outlines the variety of RFID applications that may benefit businesses, individuals, and the public and private sectors. Advantages of using RFID technology seem obvious. However, the deployment of the technology does not come without its potential drawbacks. Of particular concern is the need to establish public trust and confidence in the development of RFID applications.

EPIC therefore recommends that:

The introductory paragraph should more clearly show the conditions for RFID technology to be accepted by individuals, since the commercial success of RFID technology heavily depends on their confidence in the security, responsible uses and transparency of how RFID technology will be implemented.[3]

[3] To support the argument of the need to enhance consumers' awareness of the RFID's usages see the following examples:
http://www.edri.org/edrigram/number2.3/rfidgermany, talking about the spy chips discovered in the loyalty cards; see also http://www.foebud.org/rfid/metroskandal/en, discussing the Metro Future Store at Rheinberg (Germany), that was an example for a successful testing project for the global introduction of spy-chips see also http://www.edri.org/edrigram/number3.2/football or

A. An Overview of the Technology and its Uses

The RFID Working Document presents various current and anticipated applications of RFID technology. As stated in the Document, this technology can work in different ways depending on the types of tags and readers.[4] The Document gives current examples of how RFID technology is used, such as in car keys, vehicles, tagged boarding cards for airline passengers, hospital environments for use on patients, and in retail stores.

While there are beneficial uses of RFID technology,[5] some attributes of the technology could be deployed in ways that threaten privacy and civil liberties.

i) Transportation/Distribution

The RFID Working Document suggests that RFID systems are well-suited for certain transportation applications.[6] However, in discussing the use of RFID technology in car keys there is no mention of the danger of using proprietary/non-standard encryption implementations. Serious flaws have been discovered in RFID chips used to protect cars from theft and prevent fraudulent use of SpeedPass keys[7] Research shows that even when considered secure, RFID systems remain vulnerable.[8]

EPIC therefore recommends that:

The thorough analysis of privacy and security should be carried out prior to implementing RFID technology. All sectors should address risks of deployment of the technology. The potential for exploitation of security deficiencies serves as a warning to all industries and governments that would be tempted to hastily assemble RFID-enabled systems in order to identify and/or track people as they cross borders.

ii) Healthcare

- Pharmaceuticals

---

http://www.theregister.co.uk/2005/02/08/world_cup_2006_big_brother_charges/, talking about the mega-project of surveillance exercised upon the visitors of World Cup in Germany.

[4] RFID Working Document, *supra* note 1 at 3.

[5] One key implementation involves inventory management. For more details see *infra* section on 'Retail Applications.'

[6] RFID Working Document, *supra* note 1 at 4.

[7] SpeedPass key is a small device that allows drivers to purchase gas and convenience store goods. SpeedPass uses a radio frequency system located in the gas pump or register to "talk" with the miniature transponder located in the SpeedPass device. Each device has a unique identification and security code that is transmitted to the reader when a purchase is made. Each purchase is automatically charged to the credit card linked to the SpeedPass device. For more information *see*: http://www.speedpass.com.

[8] For further discussion on this issue *see* http://rfidanalysis.org/DSTbreak.pdf that explains how students could defeat the security of a RFID device known as a Digital Signature Transponder (DST). Manufactured by Texas Instruments, DST (and variant) devices help secure millions of SpeedPass payment transponders and automobile ignition keys. The authors have revealed the security flaws in the RFID enabled products.

RFID systems are used in the pharmaceutical industry to track medicines and prevent loss and counterfeiting derived from theft during transportation.[9] This is one of the uses of RFID in which individuals are not subjected to live RFID tags and their attendant risks. Tracking of pharmaceuticals from the point of manufacture to the point of dispensing could help ensure that these critical goods are not counterfeit, that they are properly handled, and appropriately dispensed.[10]

However, this RFID application may still raise concerns about the collection of personally identifiable information such as tracking or profiling of carriers of the RIFD devices. It can lead to misuse[11] and mismanagement of their data. Information collected might be inaccurate, incomplete, or out of date. There are also concerns about lack of transparency, data subject control and, ultimately, loss of freedom.[12]

EPIC therefore recommends that:

Privacy rules should apply to most RFID applications and additional safeguards will be necessary given RFID's unique tracking capabilities. RFID tags contained on, or in, the pharmaceutical containers should be physically removed or permanently disabled before being sold to consumers. We further recommend the adoption of a "Four Tier Approach to RFID Policy."[13] In relation to the bulk distribution of products, we recommend that no personally identifiable information (PII) be collected, and that no linking be made, to specific individuals. As far as product distribution to patients is concerned, we recommend maintaining the privacy risks proportional to the collection of PII, as well as applying privacy rules such as RFID guidelines.[14] In terms of temporary identification of patients, we recommend applying the current privacy rules with an emphasis on preventing significant security breaches.[15]

- Chip Implants

Millions of RFID tags have been sold since the early 1980s. The RFID chip contains no chemicals or battery and has a life expectancy of 20 years. They are used for livestock, pets, laboratory animals, and the identification of endangered species.[16] RFID

---

[9] RFID Working Paper, *supra* note 1 at 4.
[10] CASPIAN *et al.*, Position Statement on the Use of RFID on Consumer Products, [CASPIAN Statement] available at http://www.privacyrights.org/ar/RFIDposition.html.
[11] Data could be used for other purposes adverse to the interests of the data subject such as employment, insurance, travel.
[12] For further discussion about privacy concerns in this context *see* Marc Rotenberg, "Privacy Implications of RFID in Health Care Settings," National Committee on Vital and Health Statistics (http://www.ncvhs.hhs.gov/) of the Department of Health and Human Services, Washington DC, January 11, 2005, available at http://epic.org/privacy/rfid/rfid_ncvhs1_05.ppt [Rotenberg RFID Presentation].
[13] *Ibid.* Rotenberg RFID presentation.
[14] *See, for example,* EPIC Guidelines on Commercial Use of the RFID Technology [EPIC Guidelines] at http://www.epic.org/privacy/rfid/rfid_gdlnes-070904.pdf.
[15] For the issue of permanent identification of patients, *see* the remarks *infra* section 'Chip Implants'.
[16] For further discussion on implants *see* Opinion of the European Group on Ethics in Science and New Technologies (EGE) to the European Commission, Ethical Aspects of ICT Implants in the Human Body, March 16, 2005 [EGE

tags can also be attached to the patients themselves to verify their identities, location and the exact medical procedure to be performed by hospital staff.[17] Current applications of, *e.g.*, VeriChip[18], include medical records and healthcare information (blood type, potential allergies and medical history), personal information, as well as financial information.[19]

While EPIC proposes no privacy restrictions on the use of RFIDs in bulk products not associated with specific patients, we believe that individual tracking and profiling through a chip injected under a patient's skin, poses obvious threats to privacy and civil liberties.[20]

By agreeing to have chip implanted, individuals would lose the ability to control the disclosure of personal information. Thus, the use of RFID technology in tagging patients may involve unwanted surveillance, threatening patients' privacy and dignity. The danger of living with "chips-with-everything" including oneself, is that surveillance is becoming automated on an unprecedented scale. Tracking people directly is already happening in hospitals and in the workplace. In Singapore, in the wake of the SARS [21] scare, hospitals began tracking visitors, patients, and staff in order to determine with whom a suspected SARS patient had had contact.[22]

EPIC therefore recommends that:

There should be a general prohibition of RFID chip implants. The practice of permanent identification of patient is coercive and profound and raises far-reaching ethical implications. There is also an enormous potential for abuses when using this technology on patients, especially since the information at stake (medical information) is the most sensitive. This particular RFID application raises major concerns as to the unauthorized access to medical records, mismanagement (risk of data being used for other purposes, adverse to the data subject's interest such as employment, insurance, travel) and misuse of personal data, as well as lack of transparency and loss of personal

---

Opinion] available at: http://europa.eu.int/comm/european_group_ethics/docs/issue4.pdf.

[17] RFID Working Document, *supra* note 1 at 4.

[18] *See* EPIC VeriChip webpage at: http://www.epic.org/privacy/rfid/verichip.html.

[19] In the Baja Beach Club (in Spain and The Netherlands **,** (http://www.baja.nl), people use the VeriChip™ like a credit card to speed up drink orders and payment.

[20] The FDA has recently approved the "VeriChip" (http://www.4verichip.com) based on the injection under human skin. The "VeriChip Health Information Microtransponder" is an RFID tag designed for human use; it can be embedded with a unique identification number and implanted under the skin. Doctors and other hospital staff members 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.

[21] Severe acute respiratory syndrome (SARS) is a viral respiratory illness caused by a coronavirus, called SARS-associated coronavirus (SARS-CoV). SARS was first reported in Asia in February 2003, more information available at: http://www.cdc.gov/ncidod/sars/factsheet.htm.

[22] For further discussion *see* EPIC VeriChip webpage at: http://www.epic.org/privacy/rfid/verichip.html. *See also* Josh McHugh, "A Chip in Your Shoulder: Should I Get an RFID Implant?," Slate, November 10, 2004. Another device, recently approved, is the "SurgiChip Tag Surgical Marker System," that will use RFID technology to assist surgeons during operations. Lee Bowman, "Surgeons Get High-Tech Help to Cut Errors," Seattle Post-Intelligencer, November 20, 2004.

freedom.[23] Therefore, ICT implants (such as RFID tags and chips injected under the skin (VeriChip)) should only be allowed if there are no other less invasive means of achieving the same legitimate goals.[24]

iii) Security and Access Control

According to the work done within the International Civil Aviation Organization (ICAO), RFID will also be used in passports.[25] An ICAO committee has in fact approved a recommendation indicating that all passports and other travel documents should store electronic data on "contact-less integrated circuit" chips.[26] There are already RFID-equipped passports in Malaysia and Myanmar; Singapore is implementing the same technology, while Nigeria has contracted to do the same.[27]

Privacy ramifications of electronic passports are quite obvious since travelers carrying RFID-enabled documents, may unknowingly broadcast their tag information to any RFID reader they pass.[28] However, the US State Department's Office of Passport Policy, Planning, and Advisory Services recently announced that it is ready to begin issuing biometric passports without adequate safeguards.[29] The State Department argues that it will not use encryption to protect information contained in the passport from being broadcast to any RFID reader because the information is not different from that viewable on the information page of the passport. Furthermore, it argues, encrypted data takes longer to read and requires more complicated technology, which makes it difficult to coordinate with other nations.[30]

---

[23] For further discussion *see* Rotenberg RFID Presentation, *supra* note 12.
[24] See EGE Opinion, *supra* note 16.
[25] RFID Working Document, *supra* note 1 at 5.
[26] The Contactless IC, which is the actual *data carrying part,* normally consists of an *electronic IC* and an *antenna.* The application of the Contactless IC in Machine Readable Travel Documents (MRTD), is *passive*, that is, it contains no power source of its own. When the Contactless IC is not within the range of a machine (RF) reader it is not powered and so remains inactive. *See* ICAO Annex I, Use of Contactless Integrated Circuits In Machine Readable Travel Documents, Version 4.0 5 May 2004, available at: http://www.icao.int/mrtd/download/documents/Annex%20I%20%20Contactless%20ICs.pdf.
[27] Jonathan Weinberg RFID, "Privacy, and Regulation" in *RFID: Applications, Security, & Privacy* (Simson Garfinkel & Beth Rosenberg, eds., forthcoming 2005) available at http://www.law.wayne.edu/weinberg.
[28] One of the primary concerns with using RFID chips in the new passports is that the chips can be read from a distance, which means that an individual with an adequate RFID reader could access the data on a traveler's passport were he or she to be physically close enough. For more details, *see* PC World on the RFID passports" Your Next Passport May be Electronic, but Will it be any More Secure"? Erin Biba, Medill News Service (March 21, 2005), available at: http://www.pcworld.com/news/article/0,aid,120112,00.asp.
[29] The new passports will include a radio frequency identification tag, a chip that will store all the information on the data page of the passport, including name, date and place of birth, and a digitized version of the photo passport. The RFID chip will also contain a chip identification number and a digital signature. The two numbers will be stored in a central government database along with the personal information contained on the data page of the passport, according to the proposal in the Federal Register. *See* Department of State, the Federal Register February 18, 2005 (Volume 70, Number 33) Proposed rule on Electronic Passport [DOS Proposal] available at: http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/05-3080.htm.
[30] *Ibid.* DOS Proposal.

The European Commission has also advocated a centralized database solution, storing the biometrics of all EU travel document holders. However, it has noted that further research is necessary to "examine the impact of the establishment of such a European Register on the fundamental rights of European citizens, and in particular their right to data protection.[31] Similarly, the French Government has required that any implementation of biometric techniques is systematically subject to prior agreement from its national privacy commission.[32]

There is a major potential for misuse of this technology, which has not been sufficiently assessed and may cause many potential flaws in the system, putting citizens' privacy at risk. The remote-readability of the chip, combined with the lack of encryption to protect the communication between the chips and RFID readers will make it possible for the passport to be surreptitiously read. The ICAO specification refers quite openly to the idea of a "walk-through" inspection with the person concerned "possibly being unaware of the operation."[33] 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. Concerns arise about the possibility of businesses and governments to use RFID technology to pry into the privacy sphere of individuals.[34] The same will be true for others, too, who may be tempted to set up clandestine "walk-through inspections where the person is possibly unaware of the operation." Additionally, criminals will have a useful tool for identity theft, and terrorists will be able to know the nationality of those they plan on attacking.[35]

EPIC therefore recommends that:

Unencrypted electronic passports have to be prohibited because they pose an obvious threat to individuals' privacy. We further urge the State Department and other government agencies involved in the implementation of RFID passports, to undergo a thorough assessment of the technology used. Emphasis should be put on testing the RFID readers, which are supposed to be electronically shielded,[36] as well as, the anti-skimming feature designed to prevent identity thieves from activating and reading the chip from a distance.[37] We, further recommend that governments look at how other countries handle these concerns and learn from them, even as they proceed with the

---

[31] Commission of the European Communities, "Proposal for a Council Regulation on Standards for Security Features and Biometrics in EE Citizens' Passports," Brussels: The European Commission, 2004, available at: http://register.consilium.eu.int/pdf/en/04/st06/st06406-re01.en04.pdf.

[32] French Government, "Implementation of Biometric Techniques on French Airports," (Cairo, Egypt: Presented to the ICAO summit in Cairo, 2004), available at: http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12ip024_en.pdf.

[33] The Economist on E-passports, "High-tech Passports Are Not Working," February 17, 2005 available at: http://www.economist.com/science/displaystory.cfm?story_id=3666171.

[34] RFID Working Document *supra* note 1 at 2.

[35] *See* the Economist *supra* note 33.

[36] In order for the electronic signals sending and receiving information not to be transmitted beyond the reader, passports may be wrapped in a foil case or a weave in the cover that will cloak the chip when the passport is closed.

[37] *See* DOS Proposal, *supra* note 29.

current plan.

iv) Retail Applications

RFID technology has the potential to improve in-store efficiency and streamline retailers' storage management functions. While there are legitimate interests for businesses to track products in the product supply chain, there are also must be an emphasis put on the individuals' rights not to be tracked inside stores and after products are purchased. Certain uses of RFID are less problematic than others,[38] but all may potentially jeopardize consumer privacy, reduce or eliminate customers' anonymity, and threaten civil liberties. Some applications of the technology may not only be detrimental to data protection principles, but also violate human dignity. 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 behavior in stores; read the details of clothes and accessories worn and medicines carried by customers are all examples of uses of RFID technology that give rise to major privacy concerns.[39]

The potential harmful consequences of RFID to individuals and to society should be mitigated by taking steps to protect consumers' privacy.[40] In this respect, one author has proposed four guidelines: (1) Consumers should be notified when RFID tags are present in what they're buying; (2) RFID tags should be disabled by default at the checkout counter; (3) RFID tags should be placed on the product's packaging instead of on the product when possible; and (4) RFID tags should be readily visible and easily removable.[41]

EPIC therefore recommends that:

Businesses deploying RFID technology on individual consumer products should implement strong privacy guidelines such as EPIC's RFID Privacy Guidelines.[42] EPIC's Guidelines allow businesses in the manufacturing and retail sectors to adopt the technology in a wide range of applications while protecting consumer's basic privacy interests. They require users of RFID systems to refrain from linking personally identifiable information to RFID tag data whenever possible and only with the

---

[38] For further discussion on RFID's applications *see*, *inter alia*, Carol Sliwa and Bob Brewin, "RFID Tests Wal-Mart Suppliers," Computerworld, April 5, 2004 available at: http://www.computerworld.com/softwaretopics/erp/story/0,10801,91913,00.html; David Ewalt, "Gillette Orders 500 Million RFID Tags," Information Week, January 6, 2003 available at: http://www.informationweek.com/story/IWK20030106S0007; "Michelin Introduces Radio Frequency Tire Identification Technology," Motor Trend, January 16, 2003 available at:http://www.motortrend.com/features/news/112_news011603_tire.

[39] RFID Working Document *supra* note 1 at 2, *see also*, David Cronin, "Consumer Spy Chips Violate Human Dignity", European Voice (February 24, 2005) available at: http://www.european-voice.com/archive/issue.asp?id=435.

[40] CASPIAN Statement, *supra* note 10.

[41] Declan McCullagh, "RFID tags: Big Brother in Small Packages", CNET News.com, January 13, 2003, available at: http://news.com.com/2010-1069-980 325.html.

[42] *See* EPIC Guidelines, *supra* note 14.

individual's written consent. The EPIC Guidelines also prohibit the tracking or profiling of individuals via RFID in the retail environment; require tags and tag readers to be clearly labeled; and stipulate that tag reading events be perceptible to the consumers through their association with a light or audible tone.[43] Moreover, RFID tags should not be affixed to individual consumer products until an assessment of the technology takes place. Second, RFID implementation must be guided by Principles of Fair Information Practice. Third, certain uses of RFID should be flatly prohibited.[44] Furthermore merchants must be prohibited from forcing or coercing customers into accepting live or dormant RFID tags in the products they buy. RFID should never be employed in a fashion to eliminate or reduce anonymity. For instance, RFID should not be incorporated into currency.[45] Instead, retailers should introduce clear labeling and easy removal of tags to ensure that consumers receive proper notice of RFID systems and are able to confidently exercise their choice whether or not to go home with live RFID tags in the products they own.[46] In addition, there should be no prohibition on individuals to detect RFID tags and readers and disable tags on items in their possession.[47]

We would also like to stress the need for accountability. The consumers should be able to file complaints with designated government and industry officials regarding RFID users' noncompliance with stated privacy and security practices.[48]

B. Data Protection and Privacy Implications

Looking at data protection implications, the RFID Working Documents sets forward several examples. First, where a store can track not only the object containing the tag, but link this object to the customer's record (through store or credit card data). Second, travel passes using RFID enable the operator "to know where an identified individual travels at all times."[49] More than once the report emphasizes that: "RFID systems are very susceptible to attacks" because a third party will only need to obtain a "reader" to access the same information.

However, there is no a clear statement in the Document in favor of contact-based chips whenever personal data is processed using RFID technology. The Document acknowledges that RFID systems are very susceptible to attacks. Therefore, in order to prevent an attacker from working remotely, it should more clearly argue for the need to refrain from contactless and non-line-of-sight RFID systems. The data subject should be able to keep control over her personal data each time it is being read by RFID readers.

---

[43] Cédric Laurant testimony before Subcommittee on Commerce, Trade, and Consumer Protection, July 14, 2004 [Laurant's Testimony],
available at: http://energycommerce.house.gov/108/Hearings/07142004hearing1337/Laurant2152.htm.
[44] *See* CASPIAN Statement *supra* note 10.
[45] *See* John Leyden, "Japan Yens for RFID Chips", The Register (July 30, 2003), http://www.theregister.co.uk/2003/07/30/japan_yens_for_rfid_chips/; Winston Chai, Radio ID chips may track banknotes, News.com, May 22, 2003, http://news.com.com/2100-1017-1009155.html (EU).
[46] *See* EPIC Guidelines, *supra* note 14.
[47] *See* CASPIAN Statement, *supra* note 10.
[48] EPIC Guidelines, *supra* note 14.
[49] RFID Working Document, *supra* note 1 at 6-7.

Moreover, it is necessary to prevent a system attacker from being able to conduct passive readings of data subjects' personal information.

Furthermore, each RFID reader is simultaneously a data-collection instrument - gathering information from each RFID that responds to its broadcast - and a transmitter or broadcaster of information, as it sends its data through the information network. The databases connected to these networks hold, use, and disclose the gathered information. In such a context, the information may be used for wholly different purposes than those considered by the party that installed the RFID device, and is likely not to be apparent to the carrier of the device.[50]

EPIC therefore recommends that:

It is important to design sensor systems, including RFID systems, so that individuals are able to exercise control over the disclosure of personal information including data that would reveal actual identity. We recommend the use of contact-based chips that would minimize the likelihood of unauthorized read-out. In the case of RFID, there are a variety of technical design choices that would protect privacy. RFID-chips transmitting personal data should be either contact-based (*i.e.*, where a data subject touches a reader with the chip, which in turn allows her to know about the data processing taking place at this very moment). Alternatively, a data subject passes by a reader and a signal, for instance a green light, tells her that data processing has occurred.[51]

RFID chips transmitting personal data raise the same security issues, which apply to other wireless technology. In order to prevent unauthorized read out, it is better to place control upon the data subject carrying the chip and require an active motion (holding it onto the reader).

We further recommend the need to address the privacy threats through the system of legal controls on information use and sharing, based on a core of data protection principles such as DP Directive's Principles, Fair Information Practices.[52] Data protection law provides for many regulations and rules to be applied to data management. In the privacy context, it is useful to find the overall content of legal restraints on information use and sharing in what are commonly described as Fair Information Practices[53] or the

---

[50] *See* Stephanie Perrin "RFID and Global Privacy" in *Security and Wireless Privacy*, Simson Garfinkel ed., forthcoming publication of Addison Wesley, to be published June 2005, New Jersey, available at: http://anonequity.org/en3/index.html, at 103.

[51] *See also* discussion, i*nfra* section 'Data Security.' For further discussion on this issue *see* Weinberg, *supra* note 27.

[52] Weinberg, *supra* note 27 at 13.

[53] The Federal Trade Commission's 1998 Privacy Online: A Report to Congress identifies five such core principles: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and(5) Enforcement/Redress, see the U.S. Federal Trade Commission, Privacy Online: A Report to Congress (1998), available at: http://www.ftc.gov/reports/privacy3/.

principles set out in by OECD Privacy Guidelines.[54] Such principles make clear the rights and responsibility in the collection and use of personally identifiable information.

However, it should always be kept in mind that the best means to reduce the risk of misuse of personal information is to limit data collection in the first instance. European privacy experts are calling for collection limitation or data scarcity[55] - the "forgotten principle" - to be more respected. In the RFID context, this argues strongly for the need to avoid the adoption of tags that contain personally identifiable information or that can be linked to unique individuals.

C. Application of EC Data Protection Legislation to Information Collected through RFID Technology

The RFID Working Paper provides for a good review of the requirements of the EC Data Protection Directive (the "DP Directive") with respect to the processing of data through RFID technology. It also provides an overview of the application of the DP Directive and its principles. It addresses the question on whether specific RFID applications entail a processing of personal data, as defined in the DP Directive.[56]

Special categories of data are likely to be processed if drugs or certain consumer goods (books, films) are tagged and then combined with personal information. However, it must be kept in mind that these specific RFID applications are not allowed under Article 8 (1) of the DP Directive, provided that they do not fall under the exemption of Article 8 (2). Article 8 (2) provides that the prohibition of processing personal data can be waived in a few enumerated instances. The prohibition does not apply when the data subject has given his explicit consent to the processing of those data, or processing is necessary for the purposes of carrying out the obligations and specific rights of the controller, or to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent.[57]

Consent is the only legal ground to legitimize the collection and processing of data under Article 7 of the Directive. The matter of data subject's consent is discussed in the RFID Working Document. However, we believe that the RFID Working Document does not sufficiently address the problem of transfer of tagged goods to third parties who have not given any informed consent, and might not even be aware of the existence of the tag in situations where the tagged good comes to their possession. The major problem is

[54] In 1980, these principles were adopted by the Organization for Economic Cooperation and Development (OECD) and incorporated in its Guidelines for the Protection of Personal Data and Transborder Data Flows. They were adopted later in the EU Data Protection Directive of 1995, with modifications. *See* http://www.oecd.org/dsti/sti/it/secur/prod/priv-en.htm.

[55] The Principle of collection limitation provides that there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

[56] RFID Working Document, *supra* note 1 at 8.

[57] DP Directive, Article 8(2), *supra* note 2.

that consent cannot be obtained in scenarios where communication between RFID readers and RFID tags is taking place without the person's knowledge.[58]

EPIC therefore recommends that:

The RFID Working Document should address the problem of transfer of chipped-goods to third parties and the subsequent problem of determining whether consent exists. Individuals who carry the RFID devices may not have a chance to give a meaningful consent in many other instances.[59]

We further recommend that the only way for RFID applications to comply with the law, to the extent that these applications entail the processing of personal data, is for them not to contain personal information in the first place. In addition, there must be a way to destroy the consistent pseudonymity in order to avoid the proxy problem.[60]

Furthermore, passive tags should not be used at all in conjunction with a system that is processing personal data, since their very existence is detrimental to the limitation principle in Article 6 (1) (e) of the DP Directive.[61] Passive tags cannot be disabled in a different manner than by removing the tag itself, which entails that whenever the identification of the passive tag is linked to a data subject's personal information, the collection of personal data by any reader may be endless.

D. Technical and Organizational Requirements

i) **Standardization**

The RFID Working Paper addresses standardization bodies and their responsibility towards designing privacy compliant technology in order to enable deployers of the technology to carry out their obligations under the DP Directive.[62]

The RFID Working Paper provides standardization bodies with clear guidelines about what needs to be done to improve and safeguard data protection and privacy, and what this means for technical specifications.

However, the likelihood of providing uniform standards is fairly low, given the effort that must be put into designing and implementing a system that deals with

---

[58] *See* Perrin, *supra* note 50 at 113.
[59] While they carry their ID card to work or check at the hospital. For further discussion *see* Perrin, *supra* note 50.
[60] An example of tracking by proxy is a pet-tracking tag, which gives pet's owner's name, address, and phone number, or a number that is matched in a database to his/her personal information, Perrin, *supra* note 50.
[61] Article 6 (e) DP Directive provides that: Member States shall provide that personal data must be: kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
[62] RFID Working Document, *supra* note 1 at 11-13.

encryption, signing, verification and decryption of data on such devices. For instance, it is not certain whether the Chinese market will adopt one of the standards[63] and will not develop its own standards.[64] EPIC supports the view that there is an important role for standardization bodies to play. It will also be very important for the uniform application of data protection principles.

EPIC therefore recommends that:

Standards are needed in terms of deactivation of the tag as well as encryption of any personal data stored in the chip's memory. In addition to ISO standards for encryption and security, there should be discussion of "best practices," which are as important as the type of encryption specified by the aforementioned ISO standards. That is to say, when dealing with security and encryption, it is often more important to consider the "hows" of implementing a secure system than it is to formalize the technical specifications.

ii) **Data Security**

Database security is a critical aspect of analysis of privacy concerns associated with the RFID technology applications. It is an important issue, especially in the manufacturing and retail environment.[65] Rather than concentrating on how information may be collected via RFID devices, the focus should be on how such data is stored and whether it is adequately protected.[66] Moreover, security measures will be much more important if databases contain information from RFID tags linked to purchasers' personally identifiable information.

Technology may play a key role in ensuring compliance with data protection principles. The RFID Working Document calls for implementation of standard authentication protocols as generally the most secure approach to ensure data security.[67] In order to protect sensitive data, the RFID Working Document suggests that standard algorithms and protocols be implemented. We believe that this is an area of concern. Proprietary security solutions raise significant problems for data security, as evidenced by the RFID-enabled Immobilizer and SpeedPass problems.[68]

Another area of concern is the issue of whether a user/consumer has the right to reject and/or terminate any RFID data collection that they may have previously consented

---

[63] For instance, standards created by The EPCglobal Network. See The EPCglobal Network: Overview of Design, Benefits, and Security §3 (2004) available at: http://www.epcglobalinc.org.
[64] RFID Working Document, *supra* note 1 at 13.
[65] *See* Radio Frequency IDentification: Applications and Implications for Consumers: A Workshop Report from the Staff of the Federal Trade Commission (March 2005) [Workshop Report].
[66] As observed by one commentator: "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." *See* Thomas Claburn, "RFID Is Not The Real Issue," InformationWeek, September 13, 2004.
[67] RFID Working Document, *supra* note 1 at 17.
[68] *See* EPIC's webpage on RFID, *supra* note 8.

to. There is no mention in the Working Document of a person's ability to not only discontinue data collection, but to have everything previously collected about them expunged.[69] According to the RFID Working Document, the holder of the RFID device has the right to view all data collected, and once viewed, is entitled to opt out or disable the tag. However, it is not clear that such data subject has the right to demand that all the data previously collected be deleted.

EPIC therefore recommends that:

The alternative wording should apply in the context of sensitive data. Instead of the serving suggestion of "...should be implemented[70]," we recommend a stronger declaration: "...must be implemented."

Moreover, a mechanism for eradicating the data previously collected from the data subject should be established. It only seems reasonable to be able to do so, since it would provide a minute degree of punitive leverage for the consumer carrying the card who may be troubled by unscrupulous or abusive use of collected data. Consumers should have a choice to destroy all data collected about them in such instances.

Furthermore, we believe that insufficient attention has been paid to the issue of general data security. Therefore, we further recommend shifting the focus on privacy concerns presented by RFID devices (*i.e.*, tags and readers) to the more important concerns related to general database security, and the issue of how data that has already been collected can now be secured.[71]

4. CONCLUSION

EPIC believes that the RFID Working Document is a very important contribution to the debate on RFID technology and its privacy implications. We appreciate the opportunity to provide comments on this report and we hope that our comments will be helpful in recognizing the importance of protecting individuals from the privacy-invasive applications of RFID technology.

As the RFID Working Document rightly points out, RFID is in continuous evolution: developments in this field occur constantly and as more experience is gained, the greater is the knowledge of the issues at stake.[72] Although technology is in constant flux it should not prevent legislative developments in this area. All basic principles of data protection and privacy law have to be complied with when designing, implementing and using RFID technology.[73] The longer policymakers wait after RFID systems are

---

[69] For instance in the scenario of canceling by a consumer her loyalty card.
[70] RFID Working Document, *supra* note 1 at 17.
[71] *See* Workshop Report, *supra* note 65.
[72] RFID Working Document, *supra* note 1 at 18.
[73] International Conference of Data Protection & Privacy Commissioners (2003) "Resolution on Radio-Frequency Identification Technology" available at:
http://www.privacyconference2003.org/resolutions/res5.DOC.

deployed, the more industry players will acquire a vested stake in the technology currently in the market, and could point to the disruptive effect regulation can have on their investment in the technology.[74]

It is important to refuse to accept the tensions between privacy and technology as a zero-sum game. We therefore urge the Working Party to join us in advocating for a truly responsive legal framework that seeks creative solutions that accommodate both the values of technology and privacy.

Marc Rotenberg
President
EPIC

Ula Galster
International Policy Fellow
EPIC

Cédric Laurant
Policy Counsel
Director, International Privacy Project
EPIC

5. REFERENCES

Official documents:

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281)

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) Official Journal (L 201), 31/07/2002

International Conference of Data Protection & Privacy Commissioners, "Resolution on Radio-Frequency Identification Technology" (2003).

Commission of the European Communities, "Proposal for a Council Regulation on Standards for Security Features and Biometrics in EE Citizens' Passports," Brussels: The European Commission, (2004).

French Government, "Implementation of Biometric Techniques on French Airports," (2004).

[74] *See* Weinberg, *supra* note 27 at 9.

United States, Department of State, the Federal Register (Volume 70, Number 33) Proposed rule on Electronic Passport (February 18, 2005).

ICAO Annex I, Use of Contactless Integrated Circuits In Machine Readable Travel Documents, Version 4.0 5 (May 2004).

Opinion of the European Group on Ethics in Science and New Technologies (EGE) to the European Commission, Ethical Aspects of ICT Implants in the Human Body (March 16, 2005).

CASPIAN *et al*., Position Statement on the Use of RFID on Consumer Products (November 20, 2003).

United States Federal Trade Commission, Radio Frequency IDentification: Applications and Implications for Consumers: A Workshop Report from the Staff of the Federal Trade Commission (March 2005).

Biometric Technology on Machine Readable Travel Documents – The ICAO Blueprint, (May 11, 2003).

United States Federal Trade Commission's 1998 Privacy Online: A Report to Congress (1998).

Academic papers and presentations:

EPIC and Privacy International, *Privacy and Human Rights: An International Survey of Privacy Laws and Developments* 115-123 (EPIC 2004) ("Radio Frequency Identification [RFID]").

Stephanie Perrin "RFID and Global Privacy" in *Security and Wireless Privacy*, Simson Garfinkel ed., forthcoming publication of Addison Wesley, (to be published June 2005, New Jersey).

Jonathan Weinberg RFID, Privacy, and Regulation in *RFID: Applications, Security, & Privacy* (Simson Garfinkel & Beth Rosenberg, eds., forthcoming 2005).

Marc Rotenberg, "Privacy Implications of RFID Technology in Health Care Settings," presentation to the National Committee on Vital and Health Statistics of the Department. of Health and Human Services, Washington DC, (January 11, 2005).

Websites:

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

EPIC's Guidelines on Commercial Use of RFID Technology at:
http://www.epic.org/privacy/rfid/rfid_gdlnes-070904.pdf

EPIC's VeriChip webpage at: http://www.epic.org/privacy/rfid/verichip.html

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

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

EPIC's Public Opinion on Privacy web page reviewing opinion polls on a regular basis at
http://www.epic.org/privacy/survey

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

Press clippings:

The Economist on E-passports, "High-tech passports are not working" (February 17, 2005).

David Cronin, C*onsumer Spy Chips Violate Human Dignity*, European Voice (February 24, 2005).

PC World on the RFID passports" Your next passport may be electronic, but will it be any more secure"? Erin Biba, Medill News Service (March 21, 2005).

Lee Bowman, "Surgeons Get High-Tech Help to Cut Errors," Seattle Post-Intelligencer, (November 20, 2004).

Josh McHugh, "A Chip in Your Shoulder: Should I Get an RFID Implant?," Slate, (November 10, 2004).

Carol Sliwa and Bob Brewin, "RFID Tests Wal-Mart Suppliers," Computerworld, (April 5, 2004).

Declan McCullagh, "RFID tags: Big Brother in small packages," CNET News.com (January 13, 2003).

John Leyden, "Japan Yens for RFID Chips," The Register (July 30, 2003).

David Ewalt, "Gillette Orders 500 Million RFID Tags," Information Week (January 6, 2003).