Identification and Tracking of Individuals and Social Networks using the Electronic Product Code on RFID Tags

Markus Hansen, Sebastian Meissner
Independent Centre for Privacy Protection Schleswig-Holstein
markus.hansen@privacyresearch.eu, meissner@datenschutzzentrum.de
https://www.datenschutzzentrum.de/

Abstract. Recent studies claim that RFID transponders containing only Electronic Product Codes (EPC) do not carry person-related data. This paper describes how to use EPCs on RFID transponders to identify individuals and track their consumer habits and locations. In addition, it is shown how these mechanisms can be used to identify social networks. An overview on legal aspects is given; in particular it is elaborated under what circumstances EPC item level tagging entails the processing of personal data thus resulting in the applicability of data protection law.

1 Introduction: The Electronic Product Code

EPCglobal Inc. is a non-profit organisation founded by GS1 (former EAN – European Article Numbering International) and UCC (Uniform Code Council), the two main barcode issuing associations.

EPC, the Electronic Product Code standardized by EPCglobal, is intended to replace EAN or UPC (Universal Product Code) numbers when RFID tags replace barcodes as identifiers on products. EPC is a set of coding schemes for RFID tags, originally developed by MIT AutoID centre.

When an EPC is read, the reading system can identify the object via internet using the Object Name Service (ONS) to locate data related to a certain EPC within the EPCglobal Network community. EPC Information Services (EPCIS) are then used to exchange available information. The EPCglobal Network aims at exchanging data in real time to allow tracking of products. EPC allows for unique identification of tagged objects (as opposed to identification of object classes with barcodes). [FABHAN06]

2 Identification of Individuals

As EPC, ONS, EPCIS and the EPCglobal Network have been designed with tracking of products as a feature, the idea to use the same infrastructure to identify and track people who have bought products with EPCs attached suggests itself.

The EPCglobal Public Policy Steering Committee FAQ states that “EPC tags do not contain any personally identifiable information about consumers. [...] The only information that is contained in the EPC tag relates to the product, not the purchaser” [PPSCFAQG]. In addition, legal examinations of RFID and EPC applications also come to the conclusion that EPCs do not allow identification of a person (c.f. [HOLBON06], p. 22).

While it is true that EPC tags only contain data related to the product, concluding that they are not person-related is missing certain aspects as (at least once sold) each item has an owner. Therefore, to show that assumptions that EPCs do not allow identification of a person are false, we have a look at biometric identification and transfer the mechanisms to identification of individuals using EPCs.

2.1 Lessons from Biometrics

Biometric identification uses non-binary functions to determine if a gathered set of characteristics matches a reference set from previous enrolment. Not all biometric information is of use for identification purposes. E.g. in case of fingerprints, the minutiae and their relative positions are regarded as highly characteristic, while plain ridges are not.

As there are variations between each gathering of a print from the same person, the set of characteristics to be compared with the reference sample is varying. In addition, there may be similarities between prints from different individuals, and it is also possible that only partial prints are available. Therefore, the “true” and “false” values of an ID test are determined by probability functions. As a result, false acceptance and false rejection rates are to be dealt with. [PFITZA05]

2.2 Classification of Products

Some products have a high probability of being used by a single person only during product lifetime, e.g. a glasses frame or a pair of shoes., while others are used once only or often by different individuals. Apart from these extreme values, there are “shades of grey”. It should therefore be possible to define a classification scheme of products reflecting the probability of always being used by the same person.

Tags containing EPCs identify what kind of object they are attached to. This information can be mapped to the before mentioned classification scheme. In addition, a serial number within EPC allows for unique item identification.

2.3 Identification: The EPC Cloud

According to the classification suggested in 2.2, it is possible to define a set of EPCs that can be used as characteristics to identify individuals. We call the set of EPCs a person reveals when being scanned his “EPC cloud”. As fingerprints, the EPC cloud will contain elements that are highly (minutiae) or less characteristic (as ridges) for identification.

A scanning system will lookup the read EPCs within ONS and retrieve related information via EPCIS or from local databases, e.g. at a shop's cash register to determine which products a customer will have to pay and which ones he had already brought with him when entering the shop.

In contrast to biometric identification, there is not just an initial enrollment, but each scan and database lookup is a kind of incremental enrollment, as new characteristics are added to or dropped from the reference set.

2.4 Consumer Habits

Again in contrast to biometric identification, the low-characteristic elements of the EPC cloud are not complicating identification, but have a certain significance themselves: As these EPCs are likely to be attached to consumption goods, they indicate consumer habits. However these EPCs will usually show up within a cloud for a rather short time frame (until consumption of related goods).

2.5 Tracking

With each scan and subsequent database lookup, a dataset containing the EPC cloud, a timestamp and the ID of the querying system (and therefore the location of the person identified by a certain cloud) will result.

Tracking of EPCs is a design feature of EPCglobal: “A fundamental principle of the EPCglobal Network Architecture is the assignment of a unique identity to physical objects, loads, locations, assets, and other entities whose use is to be tracked.” [EPCGAF05]. Therefore, EPCs will also allow global tracking of individuals by ‘following their cloud’.

Despite stating that “the only information that is contained in the EPC tag relates to the product, not the purchaser” [PPSCFAQG], EPCglobal obviously is aware of the possible privacy implications of EPC tags: “Licensing agreements for the EPC specifically prohibit its use for tracking or identifying people, except in very specific cases and with full transparency relating to patient or troop safety” [PPSCFSOV].

Furthermore it is rather irrelevant what data is encoded into a unique ID and stored in the tag, as the privacy implications arise not only from the tags but even more from the data processing systems that have information linked to that ID. To verify if data contained in an EPC tag is not relating to a purchaser, it is therefore insufficient to not also look at the data processing systems.

3 Social Networks

Apart from highly characteristic elements and single-use items, it is also of interest to analyse EPCs that interchanged from one EPC cloud to another, as this is an indicator for a connection (tie) between two individuals (nodes).

Using a classification of products similar to the one from 2.2, this will allow for a qualification of links between people and therefore for identification of social networks.

4 Infrastructure Requirements

Once RFID transponders have reached a certain market penetration, reading systems to access the data stored onto them will be common as well. As a first step, RFID readers will be installed at supermarket cashiers and other points-of-sale. As shown in 2.5, log files with item identifiers of products purchased will occur.

These readers will not only read tags on items that are yet to be paid for, but for any readable transponder the customer is carrying, as the readers will not be able to distinguish between items the customer already brought into the shop and new goods prior to a database lookup.

The EPCglobal Network provides services to identify the types of items by looking up the Electronic Product Code in a database using the Object Naming Service and then retrieve related information via EPCIS.

As mentioned in 2.5, EPC Licensing agreements explicitly prohibit the use of EPC for tracking people (with defined exceptions, proving that it is possible to do so). Licensing agreements are rather weak precautions that are more likely designed to protect EPCglobal from liability claims than consumers from privacy invasion.

Security precautions as found in EPCglobal documents have their main focus authentication and authorization when using EPCIS [EPCISFAQ] and therefore are probably not intended to secure consumer privacy, but the business model of EPCglobal. Furtheron, [EPCGAF05] explicitly states that tag level security is yet to be implemented in the future: “The EPCglobal Architecture Framework does not currently discuss how these features affect the architecture above the level of the Reader Protocol, nor is there any architectural discussion of how the goals of security and privacy are address through these or other features.”

So to implement the described scenario an attacker only needs a subscription to EPCglobal to retrieve information about certain EPCs from other community members of the EPCglobal Network, a database to store gathered data, and an initial contact to EPC clouds – and therefore people – he wants to track. In case of larger supermarkets with customer discount cards, it would further be feasible to add a name to an EPC cloud, although names are not necessary for unique identification of consumers.

5 Legal Aspects

When dealing with EPC tags one fundamental question is if data protection law is applicable. This is of particular importance because it is relevant for the lawfulness of the data processing and for the existence of legal obligations such as to inform individuals about the presence of EPC tags and readers or to enable the deactivation of tags. According to Article 3 Section 1 of Directive 95/46/EC European privacy law is only applicable if personal data are processed. The question whether personal data are concerned cannot be answered across the board but has to be examined in each individual case.

A legal definition of the term personal data is provided by Article 2 a) of Directive 95/46/EC. Pursuant to this provision personal data shall mean any information relating to an identified or identifiable natural person (the so-called data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. [ECDI4695] Thereby, the term identifiable person should be interpreted extensively.

When dealing with the applicability of data protection law in the EPC context, usually three scenarios are being distinguished:

- Scenario I: Only the Electronic Product Code is stored on the tag;
- Scenario II: Again only the EPC is stored on the tag, but within the business transaction it is linked to personal data of the customer (e. g. if paying with loyalty, credit or cash card);
- Scenario III: Not only the EPC, but also personal data are stored on the tag.

Concerning the two latter scenarios it is beyond dispute that in both cases personal data are processed and therefore data protection law is applicable. In contrast, dealing with Scenario I it is a controversial issue whether EPC item level tagging (usually) entails a processing of personal data. The following explanations will elaborate on this issue:

It is true that EPC tags only contain data related to the respective product. However, from this one cannot draw the conclusion that data protection law is only applicable if the customer e. g. pays for the product with his loyalty, credit or cash card or if personal data are stored directly on the tag.

Firstly, if a direct identification is not possible, it sometimes might be feasible to identify the customer by means of personal profiles created from consumption and interest profiles, location data and data about social networks. In particular this holds for (several) controllers that collaborate in order to combine their knowledge about customers. Additionally, CCTV and connected biometric systems could – at least theoretically – be used to identify a customer.

Moreover – and predominantly –, a person might be identifiable even though no traditional identifiers are available. As already has been extensively elaborated above, some products have a high probability of being used by a single person. Shops scanning and storing the EPCs of such products are able to identify the customer wearing or carrying these products every time he enters the shop. This allows them to set up a profile of the customer and to track what (additional) items he carries with him on subsequent visits. By acting in this manner, shops are processing personal data and thus data protection law is applicable [ART29WP].

As one has to act on the assumption that an increasing number of objects will be tagged with EPCs in the future, tracking via "EPC clouds" will become an easy task and thus EPC item level tagging usually will entail a processing of personal data.

6 Conclusion

RFID transponders with EPCs on them used as tags on everyday use products allow for identification of individuals. EPCs on RFIDs allow a new type of privacy invasion: E.g. it is not neccessary any more to know the names of individuals to identify, track, and target them for advertising.

As legal regulation inherently can not prevent misuse, but just sanction it, the technical designs of systems have to provide precautions to protect the privacy of individuals by enforcing purpose-binding and deletion of collected data, and to prevent misuse by private or public entities.

As of now, license agreements seem to be the only – insufficient – protection against the described scenario.

7 References

[ART29WP] ARTICLE 29 Data Protection Working Party: Working document on data protection issues related to RFID technology, 19 January 2005, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

[EPCGAF05] EPCglobal: EPCglobal Architecture Framework Final Version, 2005, http://www.epcglobalinc.org/standards/Final-epcglobal-arch-20050701.pdf.

[EPCISFAQ] EPCglobal: Electronic Product Code Information Service Frequently Asked Questions, 2007, http://www.epcglobalinc.org/standards/FINAL-EPCIS_FAQ042707.pdf.

[EUDI4695] 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, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT.

[FABHAN06] Benjamin Fabian, Markus Hansen: Technische Grundlagen des Ubiquitous Computing, in: ULD, HU Berlin: TAUCIS – Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, Studie im Auftrag des BMBF, 2006, https://www.datenschutzzentrum.de/taucis/ita_taucis.pdf.

[HOLBON06] Bernd Holznagel, Mareike Bonnekoh: Rechtliche Dimensionen der Radiofrequenz-Identifikation, Untersuchung im Auftrag des Informationsforums RFID, 2006, http://www.info-rfid.de/downloads/rfid_rechtsgutachten.pdf.

[PFITZA05] Andreas Pfitzmann: Biometrics - how to put to use and how not at all?, Talk at ISC 2005, 2005, http://dud.inf.tu-dresden.de/literatur/Duesseldorf2005.10.27Biometrics.pdf.

[PPSCFAQG] EPCglobal Public Policy Steering Committee: Frequently Asked Questions on Guidelines on EPC for Consumer Products, no date given, http://www.epcglobalinc.org/public/ppsc_faq/.

[PPSCFSOV] EPCglobal Public Policy Steering Committee: Fact Sheet Electronic Product Code – An Overview, no date given, http://www.epcglobalinc.org/public/ppsc_factsheets/epc_overview.