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 an Electronic Product Code (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 of the relevant legal aspects is given; in particular the article elaborates under what circumstances EPC item level tagging entails the processing of personal data, thus resulting in the applicability of data protection legislation.

1 Introduction: The Electronic Product Code

EPCglobal Inc. is a non-profit organisation founded by GS1 (formerly EAN – European Article Numbering International) and Uniform Code Council (UCC), 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 Radio Frequency Identification (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 the 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 Frequently Asked Questions (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, to conclude that these data are not person-related means missing certain aspects such as 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. For example, 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 varies. In addition, there may be similarities between prints from different individuals, and it is also possible that only partial prints[1] are available. Therefore, the "true" and "false" values of an identification (ID) test are determined by probability functions. As a result, false acceptance and false rejection rates need to be handled. [PFITZA05]

2.2 Classification of Products

Some products have a high probability of being used by a single person only during the product's lifetime, e.g. a frame for a pair of glasses, 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

[1] For an example of severe problems resulting from false positives due to latent/partial prints c.f. http://en.wikipedia.org/wiki/Brandon_Mayfield.

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 that a person reveals when being scanned as his or her “EPC cloud”. As fingerprints, the EPC cloud will contain elements that are highly characteristic (such as minutiae) or less characteristic (such as ridges) for identification.

A scanning system will look up 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 customers will have to pay for and which ones they had already brought with them when entering the shop.

In contrast to biometric identification, there is not just an initial enrolment. Rather, each scan and database lookup is a kind of incremental enrolment, 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 do not complicate identification, but have a certain significance themselves: As these EPCs are likely to be attached to consumer goods, they indicate consumer habits. However these EPCs will usually show up within a cloud for a rather short time frame (until consumption of the related goods occurs).

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

2.6 Social Networks

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

When a unique EPC appears with a different EPC cloud than it has been with before, an interaction (sale, gift, theft, …) between the two individuals identified by their clouds is probable. Analysing the data that can be collected as described in this paper, it is feasible to assume that patterns of cloud hopping will be found that are characteristic and can therefore be mapped to types of interaction and social relation.

This will allow for a qualification of links between individuals and therefore for identification of social relationships such as family, friendship, employment, etc., that in combination – at least partially – represent their social networks.

3 Infrastructure Aspects

Once RFID transponders have reached a certain market penetration, reading systems to access the data stored onto them will become common as well. As a first step, RFID readers will be installed at supermarket cash desks 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. The readers will not be able to distinguish between items that the customer already brought into the shop and new goods in the store itself prior to a database lookup.

The EPCglobal Network provides services to identify the types of items by looking up the EPC in a database using the ONS and then retrieve related information via EPCIS.

As mentioned in 2.5 in relation to tracking, 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 to be designed to protect EPCglobal from liability claims than to protect consumers from privacy invasion.

The security precautions found in EPCglobal documents have as their main foci authentication and authorization when using EPCIS [EPCISFAQ]; they are therefore probably not intended to secure consumer privacy, but rather the business model of EPCglobal. Further on, [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[ed] through these or other features."

So, in order to implement the described scenario an attacker only needs the following items: 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 individuals – he or she wants to track. In case of the larger supermarket chains with customer discount cards, it would further be feasible to add a name to an EPC cloud, even though names are not necessary for the unique identification of consumers and the resulting privacy invasion.

4 Legal Aspects

When dealing with EPC tags, one fundamental question is if the current data protection legislation is applicable. This is of particular importance because it is relevant for the lawfulness of the data processing and for the existence of certain legal obligations, such as informing individuals about the presence of EPC tags and readers or enabling 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 of whether personal data are concerned in relation to RFID and EPCs cannot be answered across the board, but has to be examined in each individual case.

4.1 Introduction to the Concept of Personal Data

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). In the sense of this provision, 'identified' means that a person who belongs to a group of persons is distinguished from all other members of this group [ART29WP136] whereas 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 (or her) physical, physiological, mental, economic, cultural or social identity [ECDI4695]. Even if the name is the most common identifier, this definition implies that knowledge of the name of an individual is not an indispensable precondition to identify that person [ART29WP136]. This understanding is underpinned by a judgement of the European Court of Justice in which the court elaborates that "the act of referring, on an internet page, to various persons and identifying them by name or by other means … constitutes the processing of personal data" [ECJ03]. To assess whether a person is identifiable, one has to be aware of Recital 26 of Directive 95/46/EC which stipulates that "account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person" [ECDI4695].

4.2 The Concept of Personal Data within the EPC Context

When dealing with the applicability of data protection legislation within the EPC context, three scenarios are usually distinguished:

- Scenario I: Only the Electronic Product Code is stored on the tag;
- Scenario II: Again only the Electronic Product Code is stored on the tag, but within the business transaction it is linked to personal data of the customer (e. g. if paying with a loyalty, credit or cash card);
- Scenario III: Not only the Electronic Product Code, but also other 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 legislation is applicable. In contrast, when dealing with Scenario I, it is a controversial issue whether EPC item level tagging (usually) entails a processing of personal data [KOSVAN06]. There are a number of explanations which elaborate on this issue:

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

When focussing on EPC clouds, and considering the above explanation on the concept of personal data, one has to be aware of the fact that a person might be identifiable even though no traditional identifiers are available. As has already been elaborated in 2.2, some products have a high probability of being used by only a single person. Shops scanning and storing the EPCs of such products, and that subsequently identify a customer's EPC cloud, can easily recognize the customer every time he/she enters the premises. This means that such stores are able to distinguish this person from all other customers visiting them, and are thus able to identify the person by using his/her EPC cloud as a key for identification.

Shops are able to use the customer's EPC cloud for tracking consumption habits, and thus for setting up a consumer profile. By acting in this manner, shops are processing personal data. Thus, data protection legislation 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. EPC item level tagging will usually entail a processing of personal data, and thus data protection legislation will be applicable.

4.3 Consequences

The applicability of data protection legislation in particular leads to the following consequences:

- Personal data may only be processed if this can be based on one of the legal grounds for processing listed in Article 7 of Directive 95/46/EC (e.g., the data subject's unambiguously given consent);

- Further processing which is incompatible with the purpose of collection is prohibited (cf. Article 6 (1) (b) of Directive 95/46/EC);
- According to Article 10 of Directive 95/46/EC, the data controller must provide certain information to the data subject (particularly the controller's identity and the processing purposes);
- The data subject has the right of access i.e., of checking the accuracy of the data and ensuring that the data are kept up to date (Article 12 of Directive 95/46/EC);
- Finally, pursuant to Article 17 of Directive 95/46/EC, the data controller is obliged to implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or unauthorised disclosure.

5 Conclusions

RFID transponders with EPCs on them that are used as tags on everyday use products allow for the identification of individuals. EPCs on RFID tags allow a new type of privacy invasion: it is no longer necessary to know the names of individuals to identify, track, and target them for advertising purposes.

As legal regulation inherently cannot prevent misuse, but just sanction it, the technical designs of systems will 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, licensing agreements seem to be the only – yet insufficient – protection against this scenario.

6 References

[ART29WP105] ARTICLE 29 Data Protection Working Party: WP 105 - 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

[ART29WP136] ARTICLE 29 Data Protection Working Party: WP 136 - Opinion 4/2007 on the concept of personal data, 20 June 2007, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

[ECJ03] Judgement of the European Court of Justice C-101/2001of 6.11.2003 (Lindqvist).

[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.

[ECDI4695] 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.

[KOSVAN06] Eleni Kosta, Michael Vanfleteren: Data Protection legislation, in: FIDIS - Future of Identity in the Information Society Deliverable 7.7: RFID, Profiling, and AmI, 2006, http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.7.RFID_Profiling_AMI.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.