Data protection: multi-application smart cards: the use of global unique identifiers for cross-profiling purposes – Part I[1]

Ewout Keuleers and Jean-Marc Dinant, University of Namur (Belgium)

This article, consisting of three parts, will comment on how the opportunities offered by multi-application smart card schemes can be reconciled with data protection requirements. In the first part, the focus will be on the regulatory framework of the smart card manufacturer and the legal requirements to develop less privacy-killing technologies. Hereafter, some technical solutions will be proposed to demonstrate that multi-application smart card technology can be reconciled with the principles of personal data protection legislation. In the third and final part, the communication of personal data through electronic communications networks will be analysed. In relation hereto, it must be indicated that intelligent servers will become increasingly important to assure the interoperability between different application providers and different smart card schemes.

Multi-application smart cards are becoming more and more common

A. Introduction

Multi-application smart cards are becoming more and more common. In order to take benefit from the opportunities offered by multi-application smart card schemes, e.g., the more efficient provision of services or the generation of value-added information, authorities at different tiers are considering, or are underway, to implement local and national smart card schemes. However, from a privacy point of view, the use of such "universal" cards, incorporating various applications, e.g., financial, e-ID,[2] public transport, library, leisure, loyalty schemes etc., is not without concerns.

Based upon the personal data collected and processed via this single card, application providers or the card issuer can make a detailed cross-profile of each card holder. Although cross-profiling is not unlawful by definition and an analysis of the collected data can be legitimate, it is clear that such technologies can also be used for other purposes. To avoid the creation of George Orwell's *1984 Big Brother*, the implementation and exploitation of multi-application smart card schemes must respond to some basic preliminary requirements. In particular, attention must be paid to the use of so-called global unique identifiers (GUI). To facilitate the cross-profiling of card holders, i.e., data subjects, application providers are keen to use a unique identifier, e.g., the smart card serial number, to identify the same card holder in different scheme applications.

B. The multi-application smart card scheme

A mono-application smart card scheme is a fairly simple one, consisting of one single linear relationship, e.g., between a customer and his bank. In such a scheme, there is no interaction with applications other than those of the application provider, e.g., the card holder's financial institution.[3] In this hypothesis, it would be more difficult to make a cross-profile of the card holder, because no common identifier is used in the different databases of each application provider. For this reason, it will be more difficult to connect the different databases and make a profile of a data subject.

In contrast herewith, the architecture and the underlying privacy issues of multi-application smart card schemes are more complex. Not only should one assess the individual role of each actor involved, *e.g.*, as a data controller or data processor, but proper attention must also be paid to the inherent risk of cross-profiling. In order to facilitate the provision of certain services or to create value-added information, the smart-card-embedded application providers will share their data, *e.g.*, by transferring them to a central data warehouse.

Although multiple examples can be given of a justifiable application of cross-profiling, it is evident that such architectures can be used for less legitimate, even illegal purposes. Therefore, proper attention has to be paid to legal principles in the field of personal data protection,[4] notably to the responsibilities of each actor and to the use of global unique identifiers (GUI).[5]

The implementation of global unique identifiers in various communication devices, or in

substantial parts of it, is becoming a major privacy concern.[6] An eloquent illustration of the use of global unique identifiers is the Ipv6 protocol.[7] In this protocol a field of six bytes is foreseen within the new IP address for identifying the telecommunication terminal. By default, it seems that many Ipv6 stacks will systematically copy this serial number. As a concrete result and by side effect, the Ipv6 address will contain a "super cookie", tracking and following the user throughout every Internet communication. Furthermore and in contrast with a permanent cookie, this ID may be used not only in the HTTP protocol, but also in other protocols such as FTP, NNTP, SMTP, IMAP, POP3, etc.

The International Working Group on Data Protection in Telecommunications concluded that the characteristics of Ipv6 imply certain privacy risks. "In particular, there are profiling issues at stake whenever a unique identifier is integrated in the IP address of each electronic communication device of the user. In such a case, all communications of the user can be linked together, in fact much more easily than by using cookies."[8]

As with low-cost radio-frequency identification (RFID) tags,[9] a unique card identifier is certainly very convenient for smart card manufacturers, notably, for security and product quality reasons, e.g., to investigate dysfunctions in the production line. Nevertheless, a side effect is that unique identifiers may, are and will be used as a "tracking identifier" by other persons than the product manufacturer.[10]

It appears that almost every smart card has such a built-in identifier, *e.g.*, the Smart card Serial Number (SSN). Moreover, every application provider in the multi-application smart card scheme is easily able to access and read it. In consequence, there is an eminent risk that this SSN becomes the key to analyse each card holder's behaviour,[11] permitting a particular entity or even each application provider to have a detailed overview of the transactions made by one of its customers.

C. Legal framework for the smart card manufacturer: towards a less privacy-killing solution?

Although application providers may express their intent not to use the SSN for cross-profiling purposes, from a security perspective such a declaration of intent is not satisfactory. For this reason smart card technology has to be developed in such a way that the rerouting of the initial purposes to, e.g., cross-profiling purposes, is technically not feasible or is subject to certain constraints.[12]

In relation hereto, reference can be made to a recommendation by the Data protection Working Party. In its opinion 7/2000 of 2 November 2000, it is stated that:

The design and selection of data processing technologies, including hardware and software, shall conform to the objective of processing no or as less personal data as possible and shall facilitate the exercise of the data subject's rights. Where possible and not disproportionate with a view to the protection intended, anonymous and pseudonymous data should be used.[13]

For this reason, the main focus will be on the smart card manufacturer, in order to see to what extent the applicable data protection legislation can have an impact on the development of less privacy-killing technology.

1. The application of Directive 95/46/EC to the smart card manufacturer

(a) The qualification of the smart card manufacturer as a data controller

In principle, the following reasoning can be brought forward:

- The Smart Card Serial Number embedded in the smart card is a personal data from the moment somebody is able to identify the card holder, i.e., a data subject. This unique number is used notably for identifying the card and is

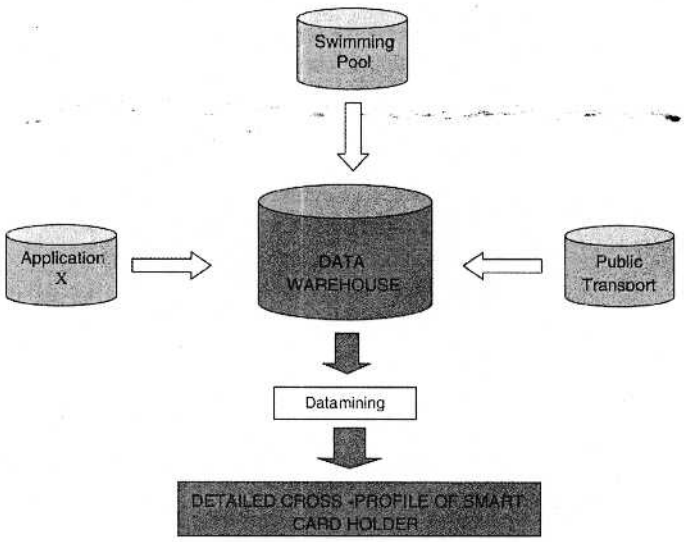

Figure 1: overview of a multi-application smart card scheme

deemed to be linked to information concerning an identified or identifiable person.[14]

- The mere storage of the SSN can be considered a processing activity.[15] In addition it must be underscored that the retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available are also considered as processing activities.
- Considering that a data controller is the person determining the purposes and the means of data processing,[16] one can defend that a smart card manufacturer is a data controller, to the extent that the latter has determined the purpose and the technical means of use of the SSN, i.e., a unique identifier.
- By virtue of article 17 of Directive 95/46/EC, the controller "has to implement technical measures to protect personal data against unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network".[17]
- The mere fact that other persons, e.g., the application providers, can read the unprotected SSN without great difficulties and therefore use it for other purposes is a major privacy issue.

It is not required that the smart card manufacturer has to identify the card holder

In this view, the mere fact that each smart card scheme application provider has an unrestricted access to the unique SSN could be considered as infringing article 17 of Directive 95/46/EC.

Nevertheless, it should be emphasised that this viewpoint can be criticised for multiple reasons.

In the first place, one has to consider that during the smart card's development or production phase, the SSN does not yet relate to any natural living person. Some authors defend an interpretation *in concreto* of the notion of personal data. According to this interpretation only data concerning an identified living natural person can be considered as personal data. In contrast, following an interpretation *in abstracto*, the identifying number can be considered as personal data in the meaning of Directive 95/46/EC because a theoretical possibility of identification exists.[18]

From the beginning on, the smart card is designated to be distributed to the public. Upon reception of the smart card, this card, including the embedded SSN, can be linked to the card holder, i.e., a living natural person. From that moment on, the SSN will no longer be an anonymous number, but will, beyond any discussion, be considered as personal data. In consequence the principles of Directive 95/46/EC have to be considered. Moreover, the initial and final purpose of the use of a SSN is to identify the person holding the card, e.g., to inform him that his card is defective. Furthermore, it should be underlined that it is not required that the smart card manufacturer has to identify the card holder. By virtue of recital 26 of Directive 95/46/EC the data controller or any other person, e.g., the card holder's financial institution, can use all reasonable means to identify the data subject.

In the second place, the qualification of the smart card manufacturer as a data controller is criticised. From a certain point of view, the smart card manufacturer only develops a technology and will offer that technology to application providers, e.g. a financial institution. The application provider will then use the technology for its particular purpose and will determine the purposes and means of its processing activities. Such a qualification, however, does not exclude the qualification of the smart card manufacturer as the controller of the information it puts on the smart cards. Indeed, it is the card manufacturer who initially takes the decision to implement a unique identifier in its cards, the purposes, e.g., for security reasons, and how this unique identifier operates. For this reason, one should make a clear distinction between the activities carried out by the application providers and those of the smart card manufacturer. In relation to each of those activities, one has to analyse the role each of the actors has. Based upon this analysis a qualification as data controller or processor can be given and the individual responsibilities of the persons involved can be defined.[19]

Considering that the qualification of data controller depends on the capacity to determine the purposes and means of data processing,[20] e.g., identification of dysfunctional cards, it can be defended that the smart card manufacturer is considered as data controller in relation to the unique identifiers such as the SSN.

(b) The qualification of the smart card manufacturer as a data processor

In some circumstances, the application provider will request that the smart card it intends to purchase, should meet certain functional and technical requirements, e.g., that they can be identified. In this hypothesis, the smart card manufacturer will give a unique identifying number to each smart card on behalf of the application provider, i.e., the data controller.

(

definition, the action undertaken by the card manufacturer cannot be considered as a processing activity for the mere reason that its activity was not performed upon personal data. Accordingly, the smart card manufacturer cannot be qualified as a data controller or processor.

Nevertheless, two arguments can be developed to counter this point of view. On the one hand and by virtue of recital 26, anonymous data are information from "which identification of the data subject is no longer possible".[26] In this regard, anonymous data should be considered as only those data that cannot identify the data subject, not now and not in the future. In this light the question remains: can data be considered as anonymous in the strict meaning of recital 26, when they are intended to identify a data subject, i.e., the card holder?

By definition, the action undertaken by the card manufacturer cannot be considered as a processing activity

Based upon section 3(6) of the Federal German Data Protection Act,[27] the following information can be considered as anonymous data: all information concerning personal or material circumstances that no longer, or only with a disproportionate amount of time, expense and labour, can be attributed to an identified or identifiable individual. Considering the proper function of a GUI, i.e., to identify people, it seems difficult to sustain that the smart card holder can only be identified with a disproportionate amount of time, expense and labour. A similar reasoning can be made for cookies. In most of the hypotheses, cookies are meant to identify a person and his web navigating preferences, e.g., the language in which a site has to be displayed.[28]

On the other hand, one must refer to the higher legal grounds on which Directive 95/46/EC was adopted and to which it specifically refers. In its recital 10 it is clearly stated that:

The object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law.

Article 8 guarantees the protection of private and family life, and interference is subject to strict conditions, i.e. in accordance with the law and is necessary in a democratic society to protect certain fundamental interests. Therefore, even if the qualification of the smart card manufacturer is not without problems, one has to consider the more universal right to privacy. Even if the actions undertaken by the smart card manufacturer do not enter the field of application of Directive 95/46/EC, the unconditional and widespread use of GUI could be considered as an unlawful interference with one's private life.[29] In addition, Directive 95/46/EC is contemplated by other legal European instruments that can offer an alternative ground to foster the development of less privacy-killing technologies.

2. The application of Directive 99/05/EC to the smart card manufacturer

Such an alternative could be offered by Directive 99/5/EC on radio and telecommunications terminal equipment.[30] Its article 2 defines terminal equipment as:

A product enabling communication or a relevant component thereof, which is intended to be connected directly or indirectly by any means whatsoever to interfaces of public telecommunications networks.[31]

The same Directive grants the European Commission the competence to decide, according to the procedure set out in article 15,[32] that an apparatus shall be so constructed that it incorporates safeguards to ensure that the personal data and privacy of the user or the subscriber are protected.[33] In application of article 2(a) of Directive 99/5/EC apparatus means any equipment that is either radio equipment or telecommunications terminal equipment or both. In this regard, there is in our view no reason for considering this Directive as not applicable to a multi-application smart card scheme, in particular to the hardware used therein.[34] [35]

Furthermore, similar provisions have been prescribed in Directive 2002/58/EC on privacy and electronic communications.[36] According to its recital 46 and article 14, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data. In recital 26 it is stated that:

Directive 95/46/EC covers any form of processing of personal data regardless of the technology used. The existence of specific rules for electronic communications services alongside general rules for other components necessary for the provision of such services may not facilitate the protection of

personal data and privacy in a technologically neutral way. It may therefore be necessary to adopt measures requiring manufacturers of certain types of equipment used for electronic communications services, e.g., smart card manufacturers, to construct ***their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected.*** *The adoption of such measures in accordance with Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity will ensure that the introduction of technical features of electronic communication equipment including software for data protection purposes is harmonised in order to be compatible with the implementation of the internal market.*

In contrast to the application of Directive 95/46/EC to a smart card manufacturer, the application of Directive 99/05/EC is not a concern. However, one bottleneck remains. To convince smart card manufactures to develop less privacy threatening products, e.g., conditional access to the unique smart card identifier, an initiative of the European Commission is required. In relation hereto, reference can be made to the legal framework for the so-called Digital Rights Management (DRM) technologies. In recital 57 of Directive 2001/29/EC on copyright in the information society,[37] it is stated that manufactures of

these technical means, in their technical functions, should incorporate privacy safeguards in accordance with Directive 95/46/EC.

How less privacy-threatening smart cards can be manufactured without substantially reducing the opportunities offered by a multi-application smart card scheme will be demonstrated in the second part of this article.

Ewout Keuleers is an attorney at the Bar of Brussels (ULYS law Firm) and a researcher at the Centre for Computer and Law (CRID). He can be reached at ewout.keuleers@fundp.ac.be or ewout.keuleers@ulys.net.

Jean-Marc Dinant is a computer engineer and is preparing his PhD on personal data security on the Internet. He was CRID's coordinator for the SmartCities Project. He can be reached at jmdinant@fundp.ac.be

FOOTNOTES

1This article is based on deliverable D12.7 on the legal aspects of the EC-funded SmartCities Project. The SmartCities project aimed and designed a dynamic smart card and multi-application management architecture to allow middle-sized cities to take advantage of the numerous opportunities of a smart card environment without being tied to a unique, proprietary applicative model. This IST Project involved Schlumberger Systèmes, Sema UK, Schlumberger Industries, Southampton City Council, University of Southampton, MasterCard Europe SA, Technolution, Crid, City of Goteborg, IT Innovation, and Black Sea Consulting. More information on this project can be found at http://www.smartcities.gov.uk. CRID is a research Centre for Computer and Law of the University of Namur (Belgium). http://www.crid.be.

2 See, e.g. http://www.fineid.fi concerning the Finnish electronic identification card.

3 Normally the chip providing, e.g., an e-purse application, such as the Belgian developed Proton card, will be integrated in traditional debit or credit card.

4 Cf., Chapter II of Directive 95/46/EC on the lawfulness of processing personal data.

In this regard reference can also be made to the so-called "eight enforceable principles of good practice" of the UK Data Protection Act 1998. http://www.dataprotection.gov.uk/principl.htm .

5 Hereafter referred to as GUI.

6 See, e.g., Etienne Wéry on the Intel Pentium® III processor, Etienne Wéry, Vie privée: Wintel is watching you, 12 March 1999, http://www.droit-technologie.org .

7 http://www.ipv6.org See also Jean-Marc Dinant, The arrival of the new Internet network numbering system and its major risks to data protection, ECLIP, October 2001. < http://www.eclip.org >.

8 See the annex to Article 29 WP, Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPV6, 30 May 2002, WP58. In connection with the use of GUI in cookies reference can be made to Article 29 WP, Working document "Privacy on the Internet" - An integrated EU Approach to On-line Data Protection, 21 November 2000, WP37, p.42.

9 Gillette seems to have implemented, or at least considered to do so, such an electronic tagging chip on each of its razor blades.http://www.alientechnology.com/library/pr/alien_gillette.htm. In fact, it appears that quite a lot if industrial companies have already produced such devices without considering the legal constraints on the use of such technologies. http://www.rfid.com . Also see The Guardian, Tesco tests spy chip technology, Tags in packs of razor blades used to track buyers, 19 July 2003. http://www.guardian.co.uk.

10 Transport for London (TfL) is using RFID-style chips in the new Oyster smart cards. http://www.tfl.gov.uk/tfl/oyster_about.shtml.

11 The unique identifier will be adopted as the unique identifying number in the data bases of each application provider of the card scheme and therefore become a general or global unique identifier. In this regard, reference has to be made to article 8.7 of Directive 95/46/EC. In this article it is stated that in relation to the processing of special categories of data, Member States have to determine the conditions under which a national identification number or any other identifier of general application may be processed.

12 In some countries, e.g., the United States, the social security number is also used for identification purposes.

13 Article 29 WP, Opinion 7/2000 On the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, 12 July 2000, COM (2000) 385.

14 Cf., recital 26 of Directive 95/46/EC.

15 Cf., article 2 (b) of Directive 95/46/EC.

16 Cf., article 2 (d) of Directive 95/46/EC.

17 Cf., infra on the qualification of application providers.

18.See, e.g., the decision of the Belgian Supreme Administrative Court on anonymous psychiatric data, Conseil d'Etat, Case no 84.880, 26 January 2000. http://www.raadvst-consetat.be/En/home_en.htm. For a more detailed analysis of the different interpretations of the notions personal and anonymous data, reference can be made to Etienne Wéry and Thibault Verbiest, Droit de l'Internet et la Sociécté de l'Information, droit européen, belge et français, Larcier, 2001, p. 412 – 427.

19 Jean-François Lerouge, "Data Protection – Transport: road tolling and privacy, some comments with regard to the EC Directive on data protection", [1999] 15 CLSR 381. It should be underscored that in the same multi-application smart card scheme different actors can be identified simultaneously as data controllers, this in function of the role they might play in the determination of the purpose and means of processing personal data.

20 Marie-Hélène Boulanger, Cécile de Terwagne, Thiery Léonard, Sophie Louveaux, Damien Moreau and Yves Poullet, "La protection des données à caractère personnel en droit communautaire", J.T. Dr. Eur., 1997,126.

21 Cf., article 2 (e) of Directive 95/46/EC.

22 Cf., articles 10 and 18 of Directive 95/46/EC.

23 Cf., article 17.3 of Directive 95/46/EC. 3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that: - the processor shall act only on instructions from the controller, - the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor. 4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1, shall be in writing or in another equivalent form.

24 Cf., article 6. 1 of Directive 95/46/EC.

25 Cf., recital 12 of Directive 95/46/EC.

26 Recital 26 of Directive 95/46/EC, in fine

27 Bundesdatenschutzgezets (BDSG), 1 January 2001. Section 3 of this Act contains definitions including the one of "rendering anonymous".

28 Cf., Jean-Marc Dinant, Law and Technology Convergence in the Data Protection Field ? Electronic threats on personal data and electronic data protection on the Internet, in *E-commerce law and practive in Europe*, Wood Head Publishing Limited, Cambridge, April 2001. Jean-Marc Dinant, 'les Traitements invisibles sur internet, Droit des technologies de l'information – Regards prospectifs, *Cahiers du CRID*, n° 16, Bruxelles, Bruylant, 1999, p.287. See also, Etienne Wéry and Thibault Verbiest, o.c.,p.423-424.

29 In this regard reference can be made to a similar conclusion related two Belgian cases concerning the articulation between the admissibility of evidence and the protection of one's privacy. Olivier Leroux and Yves Poullet, "En marge de l'affaire Gaia: de la recevabilité de la preuve pénale et du respect de la vie privée", *Revue générale de droit civil belge*, 2003, 163.

30 Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity, *Official Journal* L 091, 07/04/1999 P. 0010 – 0028.

31 For a definition of public (tele) communications networks reference has to be made to article 2 (d) of Directive 2002/21/EC (Framework Directive) and articles 2 (b) and (c) of Directive 2002/22/EC (Universal Service Directive). The distinction between private and public networks will be commented on in the last part of this paper concerning the communication of personal data through electronic communications networks.

32 Article 15 Regulatory committee procedure.

33 Cf. article 3.3 (c) of Directive 99/5/EC.

34 This provided that a public communications network is used for the transmission of the data between the different actors in the scheme. Cf. article 2 (b) of Directive 1999/5/EC. See also article 3 of Directive 2002/58/EC, infra.

35 It has to be underscored that the notion of terminal equipment also encompasses software. Cf., recital 26 of Directive 2002/58/EC: The functionalities for the provision of electronic communications services may be integrated in the network or in any part of the terminal equipment of the user, including the software.

36 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. *Official Journal* L 201, 31/07/2002 P. 0037 – 0047.

37 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society *Official Journal* L 167 , 22/06/2001 P. 0010 – 0019.