Paul De Hert · Serge Gutwirth · Anna Moscibroda

Legal Safeguards for Ambient Intelligence

Some Privacy Aspects

Received: date / Accepted: date

Abstract To take a full benefit of Ambient Intelligence, it is necessary to anticipate and react upon possible drawbacks and threats of the new emerging environment. The risks of new technologies should be examined in order to devise appropriate safeguards. This precautionary approach has been taken by SWAMI project which reflected on possible negative implications of AmI by constructing 'dark scenarios' showing possible technology failures. Analysis of the scenarios highlighted many possible problems, also for the legal framework. Current legislation and case law does not always address the threats of privacy sufficiently. The SWAMI consortium envisaged a number of legal safeguards that address lacunae in existing legislation. This article focuses on exploring only some of the lacunae in the privacy and data protection framework, and provides for examples of devised privacy-specific safeguards.

1 Introduction: the SWAMI project

Ambient Intelligence (AmI) undoubtedly brings a number of benefits. However, to fully take advantage of new possibilities, one needs to anticipate and react upon its possible drawbacks and threats of AmI. Risks that come together with benefits of the new technologies should be examined in order to devise appropriate safeguards. This precautionary but prospective approach has been taken by the SWAMI project (Safeguards in a World of Ambient Intelligence). SWAMI was a policy orientated research project within the Framework Six Program of European Union, focusing on social, economic, legal, technological and ethical issues of AmI, related to identity, privacy and security. The project brought together researchers from several disciplines, such as technologists, sociologists, economists and lawyers, with the aim of undertaking an interdisciplinary and holistic approach of AmI.

In general researchers and policy makers draw a very promising picture of the future of Ambient Intelligence and its benefits for the greater good, while very few (if any) are actually trying to foresee possible problems. The lack of proper risk assessment is striking. SWAMI-researchers therefore found that only promising pictures of AmI cannot be realistic, and concluded that a reflection on possible dark implications of developing technologies is needed. SWAMI did it by constructing 'dark scenarios' showing technology that does not work, or works in an unexpected way. The aim of focusing on such situations was to identify and highlight possible adverse impacts and risks of AmI.[1] The analysis of the scenarios showed that indeed, many potential problems might occur. These were conceptualized as threats and vulnerabilities.[2] Examples of such are: loss of privacy, security problems, loss of control, dependency, exclusion, victimisation, digital divide, and others. In this paper we will focus upon the issue of loss of privacy, seen form the legal perspective.

Amidst the problems identified by the Swami group there are problems that constitute a legal challenge. SWAMI legal research started with the examination of the existing European legal framework of privacy and data protection. Consecutively, these relevant European laws were applied to the 'dark scenario' situations, in order to discover and assess possible legal implications and consequences of unexpected functioning or malfunctioning of the technology. This legal analysis of the dark scenarios resulted in the identification of a number of lacunae in European law.

2 Erosion of Privacy in AmI

In Europe, the protection of the private life and home is guaranteed by a number of international treaties and declarations.[3] The most relevant is the European Convention on Human Rights (ECHR) [24] which protects privacy in its Article 8. Within the European Union framework privacy and data protection have been articulated as fundamental values in Charter of Fundamental Rights of the European

[1] For more info on SWAMI 'dark scenarios' and methodology see: Friedewald et al [15].

[2] For the distinction made between threat and vulnerability, as well as classification and list of discovered threats and vulnerabilities see: Friedewald et al [15].

[3] In particular, the Universal Declaration of Human Rights 1948 [23], Article 12; and the International Covenant on Civil and Political Rights 1966 [25], Article 17.

Union[4]. Respect for privacy and data protection is also regulated in several specific directives (Data Protection Directive [27], E-Privacy Directive [28], Data Retention Directive [29]), and national laws of the Member States.

An analysis of the SWAMI 'dark scenarios' allowed the research team to interrogate this regulatory framework against the background of an AmI environment. One of the main conclusions of such interrogation is that AmI can put the individual's privacy into jeopardy, and challenge the legal protection of privacy and personal data. This is due to increase in surveillance possibilities via cameras, chips, RFIDs and the possibility to follow our doings. Another contributing factor is the blurring boundaries between private and public. In an AmI environment various spaces and activities will overlap. The first of the four scenarios that SWAMI elaborated starts with a parent working for a security company doing most of his work in office at home [15]. At the same time, AmI will make it easier to deal with private things from the working environment (e.g. purchasing home products while being at work [15]), or at s public spaces such as parks or restaurants. Such situations result in doubt as to what extent privacy is legally protected in public spaces. It especially refers to the protection of privacy at workspaces and the limits of interference of employer into privacy of the employees. The SWAMI scenario also gives and example of constant monitoring of workers via cameras, or even implants enabling to localise them wherever they are and whatever they do [15]. The question is how to apply legal rules protecting the private home and life in an environment where there are no clear boundaries left between what is private and what is public? How to balance the individual privacy with other legitimate interests in AmI environment when the actors assume the multiple roles execute various task, and cross various spaces in the same time?[7] In its case law the European Court of Human Rights has introduced the notion of 'reasonable expectation of privacy' also within the working space. This criterion has allowed for important evolutions in legal understanding of privacy. In the case of Copland v. the United Kingdom [34] the Court ruled that controlling personal calls, emails and Internet use interfered with the rights of a European citizen. By refuting the home-work distinction on the basis of the criterion of 'reasonable privacy expectations', the Court has established a privacy framework that will be able to cope with some of the problems identified by the SWAMI research. Thus, individual can expect the protection of his privacy at public space (work), but such protection is not without the limits.[5] It remains unclear how far such protection goes, what it covers and particularly how such 'reasonable expectation' can be constructed. As it makes privacy protection dependent on contextual factors, it can actually also imply that the factual evolution and introduction of new technological devices will determine what privacy level can be 'reasonably expected'. Is it 'reasonable' to 'expect' any privacy when all our moves, doings and even fillings can be constantly monitored? Moreover, there is a lack of clarity concerning the consequences of a violation of privacy: While the European Court of Human Rights is willing to extend privacy protection to the workplaces and public places, it rejects the exclusionary rule, notably the right to have evidence obtained through privacy violations rejected by the courts.[6]

The SWAMI scenarios show that the development of monitoring technologies and the increasing concern for public safety lead to erosion of privacy: the 'reasonable expectation of privacy' turns into an 'expectation of being monitored'. This follows not only from the mere presence of surveillance technologies, but also from the extensive profiling possibilities they enable and the requests for the increased availability and inter-exchangeability of data between various systems, devices (and consequently between different spheres of one's life). In a hearing before the British House of Lords [12], Jonathan Faull, European Director-General for Justice, Freedom and Security (JLS), explained that this interconnected and interoperable world is actively sought after by the security community, willing to introduce what they call an 'Information Sharing Environment.' As Mr Faull explains, the 'Information Sharing Environment' (ISE) is an environment where "intelligence information should be shared between all the law enforcement agencies that are likely to find it useful." Such environment is perceived as a principal lesson that the US authorities, but also European Countries, have learned from 9/11.

Extensive profiling and interoperability can entail an unlimited availability of personal data, potentially infringing data protection law, and especially the purpose specification principle, which only allows processing of personal data for an explicit purpose, defined at the moment of collection of the data. Data availability and interoperability could threaten the citizens' rights by hampering privacy and anonymity.[7]

The impact of AmI upon privacy is especially visible when analysing some particular ambient technologies. Though many of them already exist for a long time (like surveillance cameras, RFID chips and implants), the major change will result from a massive deployment of such technologies in the future. RFID is a good example for an AmI application: It is a crucial tool to make communication between objects (objects and readers) possible, and it enables

[4] Articles 7 and 8 of the Charter [26]. The Charter does not have formally binding force.

[5] In Niemitz v. Germany [30], the European Court of Human Rights stated that there is no reason why the notion of 'private life' should be taken to exclude activities of a professional or business nature. In Halford v. United Kingdom [31] Miss Halford, a senior officer whose telephone calls were intercepted without warning, was granted privacy protection in her office space, although not absolute.

[6] In cases such as Khan [32] and P.H. & J.H. against the United Kingdom [33] the European Court of Human Rights decided that a violation of Article 8 ECHR had taken place, but it nevertheless accepted the use of the evidence found in violation of Article 8 ECHR in a criminal process.

[7] Fore more extensive discussion on drawback of interoperability see: Friedewald et al [15].

real-time monitoring of the environment and real-time automated decision making.

Although the use of RFID technology can provide for significant advantages, it is more than evident that the identification, profiling and monitoring capacities of RFID systems raise concerns, particularly with regards to its use in personal items. The SWAMI scenarios refer to RFID technology by giving the example of a product with an attached tag [15] enabling the identification of the individual user and her profile, in the scenario of a well-off person leaving alone. The misuse of this information triggers criminal activities against her. As far as privacy is concerned, rules of data protection apply if the data on the tag can lead to identification of the person.[8] However, a problem arises if such identification is not possible in a straightforward way, but only if the data on the tag is compared to other available data[9] or if RFID chip's serial number serves as an identifier although no connection with the real identity of the person is made (e.g. when a tag contains a unique identifier that allows to identify a person as an owner of the item[10]). Currently, no law addresses such situations, although such link is sufficient to conduct profiling activities. Moreover, no specific rules address RFID systems, except for some recent codes of conduct.[11]

To summarise, ambient intelligence puts privacy and data protection under pressure and threat. The current regulatory framework provides for general rules protecting these values, but they are challenged by AmI which exposes a number of lacunae in existing legislation. Blurring boundaries between spaces and between the social roles we undertake result in uncertainty what is private in a given situation, and whether it is protected. Massive deployment of data collection technologies increase the amount of information collected. The increase of computing power and the data mining possibilities facilitate extensive profiling. Profiling based on personal data is subject to the data protection requirements: the current regulatory framework requires the consent of the data subject for collection of data, respect for the proportionality principle (no more data then necessary) and purpose specification principle (data can be collected only for the purpose defined in the moment of collection of data). These principles, however, are difficult to reconcile with AmI, which needs information and needs profiling to be a truly intelligent environment. Requesting consent or providing extensive information to the data subject could occur burdensome for both, users and the data processors. Thus, should these principles still be respected? Moreover, the profiling based on data which do not constitute the 'personal data' escapes the safeguards of the current laws. Increasing profiling, data exchangeability and availability threaten the citizens' rights by hampering privacy and anonymity.

AmI therefore forces us to reconsider our understanding of current privacy and data protection in order to enhance our autonomy in the contexts of new emerging infrastructures. It forces us to seek more flexible ways of articulating AmI requirements and related social concerns. The need for new and AmI specific legal tools must be pondered.

3 Specific Safeguards Regarding Privacy and Data Protection

As AmI will raise serious challenges to the protection of privacy, conceiving legal safeguards has become a priority. This paper focuses only on very few particular safeguards addressing some of above identified lacunae in the privacy and data protection framework.[12] However, some regulatory safeguards do already exist. They are built upon existing legal framework of privacy and data protection. We believe the basic principles of such framework proved to be a sound and good basis for protecting the interest of individuals in AmI. Privacy and data protection articulate the distinction

[8] Data protection Directive applies in case of the 'personal data', defined as any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to a identification number or to one or more factors specific for his psychical, psychological, mental, economic, cultural or social identity (Article 2 of the Directive).

[9] That refers to a definition of 'personal data' under data protection law (see supra). It is clear that data are 'personal data' in understanding of the Directive when a tag actually stores personal data for the purpose of identification (e.g. tags in passports or IDs), or when the reference database exists allowing for establishing connection between info on a tag and an individual easily. However, taking into account increasing availability of data, computing and data mining capacities one can actually expect that it will be possible to establish such relation between information on a tag and the identity of individual even in lack of direct reference data, see: Hildebrandt, M., Meints, M [18]. In the contexts of RFID technology (and other, similar technologies), concept pf 'personal data' can be actually contested: as Article 29 Data Protection Working Party states in its Working document on data protection issues related to RFID technology [1], if processing of data collected via RFID systems is covered by the data protection Directive, we must determine whether such data relates to an individual, and whether such data concerns an individual who is identifiable or identified. In assessing whether information concerns an identifiable person, one must apply Recital 26 of the data protection Directive which establishes 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." And further: "Finally, the use of RFID technology to track individual movements which, given the massive data aggregation and computer memory and processing capacity, are if not identified, identifiable, also triggers the application of the data protection Directive."

[10] The stabile connection between the item and the individual is then necessary. It is possible to establish such link in case of personal products the owner carry with him/her. An illustration of such situation and concern was given by Article 29 Data Protection Working Party in its document on RFID [1]. Such stabile link between the item and the owner is often contested in the contexts of RFID tags. See also: Hildebrandt. M., Meints, M [18].

[11] The issue of RFID safeguards will be dealt with more extensively further in this paper.

[12] For a broader overview of safeguards to privacy see Friedewald et al [15]. The SWAMI consortium also proposed some general safeguards addressing the issues of regulating AmI, and the AmI law making, see idem.

between opacity and transparency. Opacity tools protect the individual's autonomy against the interference of the powerful actors, while transparency tools accept such interference, though under certain conditions which guarantee the control, transparency and accountability of the interfering actors and actions [9], [10], [13]. In democratic constitutional states both sorts of tools are used simultaneously. The right to privacy can be understood as an opacity tool, while data protection is an example of transparency approach [10]. As AmI is based on processing of the information, we consider that transparency tools should provide default position. Collection and processing is thus allowed (as AmI requires it), but under control of data protection principles. We think such basic safeguards of data protection should be respected, although we acknowledge that certain gaps need to be addressed, and a number of aspects need clarification (supra).

However, certain opacity measures – prohibitions of violations of privacy – shall also be enacted in order to protect individuals against unbalanced controlling and surveillance powers and discriminations. This could, for example entail surveillance-free territory for workers, restrictions on using implants, or restricted interoperability of large scale databases. As for increased interoperability and profiling, they should not be considered as purely technical issues, but also with their multiple political, legal and economical implications. There is a difference between the power to connect and process personal data, and the desirability and acceptability of those actions. Basically, personal data that were not meant to be merged and made available (at the moment of collection), should not be subjected to these operations [8], [14].

But as we already discussed, AmI will bring new dimensions, new threats and new vulnerabilities, which demand some AmI-specific safeguards. Below we discuss two examples of such targeted safeguards: digital territories that can be understood as an opacity tool, and a safeguard addressing the AmI-specific technology (RFID) combining both, opacity and transparency approaches.

3.1 Digital Territories

The concept of digital territories aims at providing the individual a secured possibility to enjoy his or her privacy in a highly networked and digitalised world, This private, digital space could be considered as an extension of the private home, and could be accessed at (any) chosen time and place. Digital territories introduce new notions of space and borders in the future digitised everyday life, but with the particularity that such virtual boundaries would be determined and controlled by the user. Thus, it may provide for the useful concept of privacy protection in a 'borderless' AmI environment. A digital territory can also be conceptualised as a sort of bubble, of which the opacity or transparency depends on the will of its subject.[13] It is a sort of 'membrane' managing the information flow to and from the user.

Already today people process their personal data on servers (files, pictures, correspondence), communicate through the Internet, disseminate personal information and content while being on-line. The engagement of the individuals into such activities will obviously only increase in the future, which will move our 'private activities' more on- line, linking our 'real' life with the 'virtual' one.

It is questionable whether the law guarantees a sufficient and workable protection of such online private spaces [3], [7], [4]. For instance, the law itself requires telecommunication service providers to keep communication data at the disposal of law enforcement agencies (data retention obligations [29]), while it is unclear whether there are any guarantees for the individual when these data are being accessed. Moreover, within the context of on-line communication, relations with private parties or institutions (e.g. commercial transactions, social networking, e-government services) the privacy of the individuals is, in principle, legally protected especially by data protection law. However, the definition of 'personal information'[14] does not distinguish between different categories of information and various levels of 'privacy' (with the exception of 'sensitive data' which are afforded stricter protection). It also imposes heavy formal requirements applicable to each data collection/disclosure (and hence each relationship), spawning many compliance difficulties for all the parties. To interact, indeed, we need to disclose parts of ourselves, but we should also be able to stay in control what is being disclosed. The concept of digital territory has the advantage to allow for such flexibility and control, leaving it to the user to decide whether (s)he discloses personal info, to whom, for which purpose and by allowing him to 'tag' private data for follow-up reasons [7].

To ensure that such virtual private territories become effective, they must be legally defined and protected. The law should protect against unwanted and unnoticed interventions by private parties or public actors, alike in the case with the protection of inviolability of the private home. A set of the legal rules could be envisaged to that end, for example procedural safeguards similar to those currently applicable to the home, e.g. requiring a search warrant. Technical solutions aimed at defending private digital territories against intrusion should be encouraged and, if possible, legally enforced [9]. Privacy enhancing technologies are an important element of such policy, and especially development of identity (information) management systems.[15] Such protection could also be

[13] See: Beslay, L., and H. Hakala [3]. In-depth analysis of the concept and various categories of digital territories can be found in recent IPTS report: Daskala, et al [7].

[14] See supra: 'Erosion of Privacy in AmI'.

[15] An overview of the existing identity management systems has been given by Bauer et al [2]; Hildebrandt M., Backhouse, J., (eds.), [17], and Müller et al [21]. Development of identity (information) management

extended to the digital movements of the person, similarly to the extension of the privacy of the home to the individual's car. The protection could also be envisaged for home networks linked to external networks.[16]

3.2 Specific Recommendations Regarding RFIDs

AmI depends on the deployment of particular technologies enabling large scale data collection and processing, but such technologies might bring particular problems to privacy. A specific safeguard addressing impacts of each particular technology is needed. Recommendations regarding RFIDs will be examined as example of such approach.[17]

The Article 29 Working Party has already given some guidelines on the application of the principles of EU data protection legislation to RFID [1]. It stresses that the data protection principles must always be complied with when the RFID technology leads to processing of personal data.[18] We share the opinion of Article 29 Working Party that rights of the data subject, as granted by data protection Directive, should still be ensured also in case of RFID systems. Therefore, the individual should always be aware of the presence of tags and readers, purpose of collecting and processing the data, who is a responsible controller, whether data (and what kind of data) are stored, the means to access and rectify data, whether they will be accessed by third parties. His consent still should be sought to legitimise data processing.

As providing such information may be fairly complicated and burdensome both for users and marketers, adequate, simplified notices informing on presence, activity of tags and readers, and the policy of the data processors should be used (e.g., pictograms or similar). Such information should always be provided to consumers when RFID technology is used, even if a tag does not contain personal data in itself.[19] The data subject should have the possibility to discharge, disable or remove a tag. It is a consequence of the consent principle of data protection, since the individual should, in principle; always have the possibility to withdraw his consent.

Privacy by design is of crucial importance in any technological applications, so also in case of RFID tags. It is thus important to continue efforts in developing technical specification and privacy standards.[20] Privacy assessment, aiming to identifying all potential risk of each particular RFID application could be a legally binding obligation [5]. The SWAMI consortium also recommends further research into RFID technology, its implications for privacy, and a further reflection on possible legal safeguards.[21] Further development of the codes of conducts and good practices were also recommended.[22]

4 General Conclusions

The SWAMI project emphasised a need for reflection on possible 'dark' sides of AmI. It also identified a number of lacunae in an existing legal framework, which often does not provide sufficient protection for AmI threats. Therefore the SWAMI consortium proposed a number of safeguards, which aim at mitigating possible drawbacks of the new environment. These particular safeguards should not be treated as a closed list. In contrary, the SWAMI project came to a more general conclusion: there is never enough of precautionary reflection, based both on analyses of particular technologies with their particular problems, as well as based on more general observations. This paper presented examples of legal safeguards to loss of privacy. The AmI-specific concept of digital territories has been presented as a concept that can ensure that individual stays in control of his/her privacy despite the blurring borders between private and public, and despite eroding privacy expectation. Specific safeguards for RFID technology were presented as an example of the precautionary reflection on particular AmI technological application. The SWAMI concluded that further research on AmI legal problems should continue. There is a need for improving existing and devising new regulatory safeguards.

References

1. Article 29 Data Protection Working Party: Working document on data protection issues related to RFID technology. 2005, (10107/05/EN WP 105). http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf, last consulted 02.07.2007.
2. Bauer M., Meints, M., Hansen, M., (eds.): Structured Overview on Prototypes and Concepts of Identity Management Systems, FIDIS (Future of Identity in the Information Society) Deliverable D3.1, 2005. http://www.fidis.net

systems have been discussed in Hansen, et al [16], Leenes et al [20], and within the FIDIS project in: Schreurs et al [25].

[16] This relates to the special case of the digital territory, the virtual residence. See: Beslay, L., Punie, Y. [4], and Daskala et al [7].

[17] More on RFID safeguard in: Friedewald et al [15].

[18] The concept of 'personal data' in Data Protection Directive might be difficult to interpret in the context of RFID technology and AmI in general. It is thus unclear whether RFID contains a personal data. See supra: 'Erosion of Privacy in AmI'.

[19] As already mentioned, such information on a tag can be a unique identifier enabling profiling activities. See: Kardasiadou, et al. [19].

[20] Some standards have already been adopted in the RFID domain. The International Organization for Standardization has developed sector-specific standards, as well as more generic standards. Some standards have also been developed by EPCglobal Ltd. http://www.epcglobalinc.org/home, an industry-driven organisation, creating standards to connect servers containing information relating to items identified by EPC (Electronic Product Code) numbers.

[21] Researchers and legislators should also seek further solutions addressing the issue of profiling enabled by such technologies. See supra: 'Dangers of AmI Enabling Technology- RFIDs'; see also: Hildebrandt, M., Meints, M., [18].

[22] An example of such (emerging) initiatives is the EPCglobal Ltd. guidelines regarding privacy in RFID technology [11], and CDT (Centre for democracy and technology) Working Group on RFID Privacy Best Practices [6].

3. Beslay, L., Hakala, H.: Digital Territory: Bubbles, 2003. (draft version available at http://cybersecurity.jrc.es/docs/DigitalTerritoryBubbles.pdf), last consulted 02.07.2007
4. Beslay, L. Punie, Y.: The Virtual Residence: Identity, Privacy and Security. In: Security and Privacy for the Citizen in the Post-September 11 Digital Age: a Prospective Overview, IPTS Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), 2003. http://ftp.jrc.es/eur20823en.pdf, last consulted 02.07.2007.
5. Borking, J.: RFID Security, Data Protection & Privacy, Health and Safety Issues. Presentation made during European Commission Consultation on RFID, Brussels, 2006.
6. CDT (Centre for democracy and technology) Working Group on RFID: Privacy Best Practices for Deployment of RFID Technology, Interim Draft, 2006. http://www.cdt.org/privacy/20060501rfid-best-practices.php, last consulted 02.07.2007.
7. Daskala, B., Maghiros, I.: Digital Territories: Towards the protection of public and private spaces in a digital and Ambient Intelligence environment. 2007, EUR 22765 EN http://www.jrc.es/publications/pub.cfm?id=1474
8. De Hert, P.: What are the risks and what guarantees need to be put in place in view of interoperability of police databases? Standard Briefing Note 'JHA & Data Protection', No. 1, produced on behalf of the European Parliament, 2006.
9. De Hert, P., Gutwirth, S.: Making sense of privacy and data protection: A prospective overview in the light of the future of identity, location-based services and virtual residence. In: Security and Privacy for the Citizen in the Post-September 11 Digital Age: a Prospective Overview, IPTS Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), 2003. http://ftp.jrc.es/eur20823en.pdf, last consulted 02.07.2007.
10. De Hert, P., Gutwirth, S.: Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. In: Claes, E., Duff, A., Gutwirth, S. (eds.): Privacy and the criminal law. 2005, Antwerp/Oxford, Intersentia .
11. EPCglobal Ltd. guidelines regarding privacy in RFID technology,http://www.epcglobal.org/public_policy/public_policy_guidelines.html, last consulted 02.07.2007.
12. Faull, J., heard by the House of Lords, Minutes of Evidence taken before the Select Committee of the European Union (Sub-Committee F), The EU-US PRN Agreement, 22 March 2007, p. 5 http://www.publications.parliament.uk/pa/ld/lduncorr/euf220307_2.pdf, last consulted 02.07.2007.
13. Gutwirth, S.: De polyfonie van de democratische rechtsstaat. [The polyphony of the democratic constitutional state]. In: Elchardus, M. (eds.): Wantrouwen en onbehagen [Distrust and uneasiness]. 1998, Balans 14, VUBPress, Brussels.
14. Gutwirth, S., De Hert, P.: Regulating profiling in a democratic constitutional state. To be published in: Hildebrandt, M., Gutwirth, S. (eds.): Profiling the European citizen. Forthcoming, 2007, Springer Press, Berlin.
15. Friedewald, M., Gutwirth, S., Punie, Y., Wright, D., Vildjiounaite, E., (eds.): Safeguards in a World of Ambient Intelligence. Accepted for publication in 2007 by Springer, Dordrecht.
16. Hansen M., Krasemann, H. (eds.): Privacy and Identity Management for Europe - PRIME White Paper - Deliverable 15.1, 2005.
17. Hildebrandt M. Backhouse, J., (eds.): Descriptive analysis and inventory of profiling practices, FIDIS (Future of Identity in the Information Society) Deliverable D7.2, 2005. http://www.fidis.net
18. Hildebrandt, M., Meints, M. (eds.): RFID, Profiling, and AmI, FIDIS (Future of Identity in the Information Society) Deliverable D7.7, 2006. http://www.fidis.net.
19. Kardasiadou, Z., Talidou, Z..: Report on Legal Issues of RFID Technology, LEGAL IST (Legal Issues for the Advancement of Information Society Technologies) Deliverable 15, (2006).
20. Leenes, R., Schallabock, J., Hansen, M.: Prime white paper v2., 2007. https://www.prime-project.eu/prime_products/whitepaper/, last consulted 02.07.2007.
21. Müller G. and Wohlgemuth, S., (eds.): Study on Mobile Identity Management, FIDIS (Future of Identity in the Information Society) Deliverable D3.3., 2005. http://www.fidis.net
22. Schreurs, W., Hildebrandt, M., Gasson M., Warwick, K., (eds.): Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence, FIDIS (Future of Identity in the Information Society) Deliverable D7.3, 2005. http://www.fidis.net

Legal Acts

23. Universal Declaration of Human Rights, United Nations, 1948.
24. European Convention on Human Rights of 4 November 1950
25. International Covenant on Civil and Political Rights, United Nations, 1966,
26. Charter of Fundamental Rights of the European Union, *OJ* C 341, 18.12.2002, pp. 1-22.
27. 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 on the free movement of such data, *OJ* L 281, 23/11/95, pp 31-50.
28. 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) *OJ* L 201, 31/07/2002, pp. 37-47.
29. Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *OJ* L 105, 13/4/ 2006, pp. 54-63.

Case Law

30. ECHR, Niemitz v. Germany (23.11.1992).
31. ECHR, Halford v. the United Kingdom (27.03. 1997).
32. ECHR, Khan v. the United Kingdom (12.03.2000).
33. ECHR, P.H. & J.H. v. the United Kingdom (25.12.2001).
34. ECHR, Copland v. the United Kingdom (3.04. 2007).