Privacy Policy Referencing*

Audun Jøsang[1] and Lothar Fritsch[2] and Tobias Mahler[3,2]

[1] UNIK University Graduate Center - University of Oslo
josang@unik.no
[2] Norwegian Computing Center
Lothar.Fritsch@NR.no
[3] Norwegian Research Center for Computers and Law - University of Oslo
tobias.mahler@jus.uio.no

Abstract. Data protection legislation was originally defined for a context where personal information is mostly stored on centralized servers with limited connectivity or openness to 3rd party access. Currently, servers are connected to the Internet, where large amounts of personal information are continuously being exchanged as part of application transactions. This is very different from the original context of data protection regulation. Even though there are rather strict data protection laws in an increasing number of countries, it is in practice rather challenging to ensure an adequate protection for personal data that is communicated on-line. The enforcement of privacy legislation and policies therefore might require a technological basis, which is integrated with adequate amendments to the legal framework. This article describes a new approach called Privacy Policy Referencing, and outlines the technical and the complementary legal framework that needs to be established to support it.

1 Introduction

Data protection law regulates the processing of information related to individual persons, including their collection, storage, dissemination etc.

Privacy concerns exist wherever personally identifiable information is collected and stored – in digital form or otherwise. Some forms of processing personal information can be against the interests of the person the data is associated with (called the data subject). Data privacy issues can arise with respect to information from a wide range of sources, such as: Healthcare records, criminal justice investigations and proceedings, financial institutions and their transactions, private sector customer data bases, social communities, mobile phone services with context awareness, residence and geographic records, and ethnicity information. Amongst the challenges in data privacy is to share selected personal data and permit the processing thereof, while inhibiting unwanted or unlawful use, including further dissemination. The IT and information security disciplines have made various attempts at designing and applying software, hardware, procedures, policies and human resources in order to address this issue. National and regional privacy protection laws are to a large extent based on the OECD data privacy principles

[*] In the proceedings of the 7th International Conference on Trust, Privacy & Security in Digital Business (TRUSTBUS'10), Bilbao, August-September, 2010.

defined in 1980 [21], e.g. the EU Data Protection Directive [13]. The legal framework for data protection has been adapted to take into account some of the changes in technology, but the constant technological change has been challenging to follow up. In the 70s and 80s personal information was stored on mainframe computers, on punch cards or on tape rolls with limited connectivity. The Internet only existed in the form of the experimental ARPANET, and no commercial applications had been conceived. It is natural that the principles defined by the OECD in 1980 reflected the computing infrastructure at that time, and the principles can be judged as relatively adequate from that perspective. Since then, the legal framework has struggled in keeping up with changes in the technology.

On the technological side, a long track of information security research exists. Their focus is the development of privacy-enhancing technology (PET) in support of the - mostly legally derived - requirements for personal information handling. A brief historical overview over privacy regulation and PET is given in [15]:

> Starting in the 1970ies, regulatory regimes were put on computers and networks. Starting with government data processing, along the lines of computerization of communication and workflows, explicit rules like the European Data Protection Directive [7] have been put in place. With the adoption of Internet and mobile telephony in society in the past decade, the privacy challenges of information technology came to everyday life.The PET research perspective focused to a certain degree on the legal foundations of privacy protection, determined by constitutional and fundamental human rights that should be protected using technology. This view is shown in an analysis of the PET vocabulary in [18]. As rights are granted to individuals, much of the research has focused on the user-side, e.g. visible in Pfitzmann/Hansen's well-quoted terminology paper [23]. The legal view is propagated into contemporary frameworks like the Canadian [22] and Dutch [28] privacy legislation, which both define privacy audit schemes with detailed procedural definitions and responsibilities, but neglect to provide a decision support method for managers that would enable them to make feasible decisions about privacy needs based on quantifiable risks. Most of these criteria, including schemes like Datenschutz-Gütesiegel [16], provide checklists with questions for the auditors. They inherently call for competent – and well-paid – external experts when they are used by a company, but are rarely based on empirical data or metrics. The PET award winning taxonomy of privacy [26] is very visibly structured along the legal view on privacy.

Many assumptions underlying traditional PETs (Privacy Enhancing Technologies) are no longer valid. Users have little control over information they provide to service providers, which e.g. exposes them to various profiling risks [14]. M. Peter Hustinx, the European Data Protection Supervisor, said in his keynote talk at NordSec 2009 [4]that the EU and OECD have recognized the erosion of the adequacy of the classic privacy principles after the emergence of the Internet. In 2009, these organizations therefore have initiated a

[4] ”Privacy in the Internet Age” URL: NordSec2009.unik.no

process for defining new and more adequate privacy principles for networked environments. Similarly, in a keynote speech at the Data Protection Day on 28 January 2010 at the European Parliament, Brussels, Viviane Reding[5] expressed the intention to present a legislative proposal for reforming the European Privacy Directive before the end of the year (2010), and launched the concept of ”privacy by design” [24] which specifies that privacy requirements must always be included in the design of new Internet technologies. In her speech she said that the new legal framework should address new challenges of the information age, such as globalisation, development of information technologies, the Internet, online social networking, e-commerce, cloud computing, video surveillance, behavioural advertising, data security breaches, etc.

Privacy policies are sometimes used by organizations that collect and process personal information. However, users often pay little or no attention to these privacy policies, and once the personal information has been collected, it is practically impossible to verify that the specified privacy policies are being adhered to. There is also scientific evidence that user-side reading of privacy policies is in conflict with basic market economic principles [30].

It can also be mentioned that the protection of personal data is sometimes in conflict with other interests of individuals, organizations or society at large. Several occasions, for example the ’war on terrorism’, showed that the European Union delivers passenger flight databases, SWIFT financial transactions, and telecommunications data to authorities outside the EU legislation. In such cases, no consent is necessary, if such disclosure is lawful under the applicable law.

From this brief survey it seems timely to rethink how information privacy should be defined and enforced in the online environment. This paper looks at the inadequacy of the current approach to information privacy protection, and proposes a new approach based on attaching policy metadata to personal information. By requiring that the metadata follows personal information, it becomes easy to verify whether the policies are being adhered to. In addition, one should consider standardizing privacy policies in the form of a limited set of easily recognizable rules to improve the usability of privacy protection.

2 The Inadequacy of the Current Approach

2.1 Business decision-making and privacy technology

For any deployment of PET into information systems, the effectiveness of the PET measure against threats is important [15]. While PET cost of installation and operation could be assessed with experiments, the efficiency of their deployment remains unknown. In the computer science field, several contributions provide information theoretic models for anonymity, identifiability or the linkability of data, e.g. in [27]or in [10]. Both papers build mathematical models that are rather impractical for usage in the evaluation of large-scale information systems. Another suggestion comes from an article on intrusion detection by user context modeling [19], where the author tries to identify attacks by classification of untypical user behavior. Such behavioral analysis

[5] Member of the European Commission responsible for Information Society and Media Privacy

can be developed into a tool to measure effectiveness of PET. From some experiments on profiling people with publicly available data from the Internet [9], one might try to use profiling output as a measure of the quality of PET systems. But the definition of the information that counts as a part of a profile, as well as the question of how to distinguish leaked information from intentionally published personal information make profiling a rather impractical metric. With these difficulties in measuring effectiveness of PET, how will we judge efficiency? Also, for the deployment of PET on the business side, or the acceptance of some extra effort by users adapting to PETs, there are more questions to ask:

- Which PET will remove or reduce a particular risk? At what cost will a particular PET remove a particular risk?
- How much effort (instruction, change of system usage habits, change of behavior, self-control) had to be spent on the user-side for the PET to be effective?
- Is there a cheaper or more convenient alternative on how to deal with a particular risk instead of PET deployment?

2.2 Inadequacy of Technical Privacy Strategies

Public surveys indicate that privacy is a major concern for people using the Internet [6]. Privacy related complaints that are made to the US Federal Trade Commission include complaints about unsolicited email, identity theft, harassing phone calls, and selling of data to third parties [20]. One attempt to address privacy concerns and thereby increase user trust in the Web is the W3C's Platform for Privacy Preferences (P3P) Project [8]. P3P enables Web sites to express their privacy practices in a standardized, XML-based, format that can be automatically interpreted by user agents such as a Web browser. The aim is that discrepancies between a site's practices and the user's preferences can be automatically flagged. Nine aspects of online privacy are covered by P3P,including five that cover data being tracked by the site: who is collecting the data; what information is being collected; for what purposes is it being collected; which information is being shared with others; and who are the data recipients. Four topics explain the site's internal privacy policies: can users make changes in how their data is used; how are disputes resolved; what is the policy for retaining data; and where can the detailed policies be found in a'human readable' form. It would be fair to say that P3P has been a failure because users and industry have not adopted it.One of the reasons might be that P3P is unable to guarantee or enforce the privacy claims made by Websites. Despite its potential, detractors say that P3P does not go far enough to protect privacy. They believe that the aim of privacy technology should be to enable people to transact anonymously [11]. Private privacy service providers or *anonymisers* have been proposed [29]. One example is iPrivacy, a New York based company that around 2002 professed on its Web site, "not even iPrivacy will know the true identity of the people who use its service". To utilize the technology, users first had to download software from the Web site of a company they trusted, for example a bank or credit card company. When they wished to purchase a product online, they used the software to generate a one-off fictitious identity (name, address and email address). Users were given the choice of collecting the goods from their local post office (their post or zip code is the only part of the address which is correct) or having the goods delivered by a delivery company or postal service that has been sent a decoded address label. Originally the iPrivacy software generated a one-off credit card number for each transaction. The credit card issuer matched the credit card number it received from the merchant with the user's real credit card number and then authorized payment. However,this proved to be a major job for banks to integrate and is no longer offered by iPrivacy. There are still other companies such as Orbiscom.com and Cyota.com (acquired by RSA) that do offer one-off credit card numbers,but these have captured limited use to date. Another type of privacy provider or *infomediary* is emerging which sells aggregated buyer data to marketers, but keeps individual identifying information private [29]. One example of this is Lumeria, a Berkley based company that provides royalties to people who participate. In the Lumeria system, users download free software that encrypts their profile and stores it on Lumeria's servers. The user accesses the Web via a Lumeria proxy server, which shields their identity from merchants and marketing companies whilst enabling marketing material that matches their profile to be sent to them. However, none of these initiatives have been a success, and many privacy providers have gone out of business. This is quite understandable, as the anonymity solutions result in significant additional complexity and cost.

2.3 Inadequacy of Specifying Privacy Policies

Many data controllers specify privacy policies that can be accessed from the interface where personal information is being collected or where consent to do so is given. Such policies are sometimes of 10 pages or longer, and can be written in a jargon that makes them inaccessible for most people. Users are normally required to accept the policies by ticking a box, which all but very few do in a semi-automatic fashion. Users quickly learn that reading such policies is very frustrating. In addition, users who might be opposed to some clauses in the policy faces the organization alone, although many others might be of the same opinion. It is difficult for users to organize themselves and exercise pressure on organizations to change their privacy policies, but both data protection authorities and consumer ombudsmen have succeeded in pressuring some organizations to change their policies. Once personal information has been collected, users have no practical way of verifying whether the policies are being adhered to. In practice, it would also be difficult to trace personal information back to the point where it was collected. Once inside the network or system of an organization, it often becomes very difficult to trace personal information back to the point of origin and the applicable privacy policy. This is precisely where our proposal offers a solution, whereby the applicable privacy policy always is referenced by the metadata associated with any personal information. This will be explained in further detail below.

The privacy policy interpretation and specification troubles are illustrated in a survey article that provides a taxonomy of 'privacy-supporting' and 'privacy-consuming' privacy clauses from real policies [1]. The survey clearly shows that most privacy policies on web pages are carefully drafted to lure the consumers into accepting privacy-consuming clauses.

A privacy policy may fulfill several different functions [4] (p.239). First, it can be used to provide information about how personal data is processed by the data controller, and such information may be mandatory according to the law. Second and somewhat related, a policy may provide the background for a statement of consent to certain forms of processing. Thus, the policy may explain what the data subject is consenting to. The existence of a privacy policy may also lead to some users increasing their trust in an organization. However, particularly regarding very lengthy, ambiguous and open privacy policies may one may sometimes suspect that the intention is not to provide clear information and rules for data processing, but rather to secure the flexibility of the data controller in processing the data in any desired manner.

However, if a privacy policy is in conflict with the applicable data protection law, then it may have a limited or no legal effect. The most important rules in data protection law can be expressed in relation to a number of basic principles [3] to be found in most international and national data protection instruments and laws.

- **Fair and lawful processing**: Personal data must be processed fairly and lawfully.
- **Purpose specification**: Personal data must be collected for specified, explicit and legitimate purposes and not further processed for other purposes.
- **Minimality**: The collection and storage of personal data should be limited to the amount necessary to achieve the purpose(s).
- **Information quality**: Personal data should be valid with respect to what they are intended to describe and relevant and complete with respect to the specified purpose(s).
- **Data subject participation and control**: Persons should be able to participate in the processing of data on them and they should have some measure of influence over the processing.
- **Limitation of fully automated decisions**: Fully automated assessments of a persons character should not form the sole basis of a decision that impinges upon the persons interest.
- **Disclosure limitation**: The data controllers disclosure of personal data to third parties shall be restricted, it may only occur upon certain conditions.
- **Information security**: The data controller must ensure that personal data is not subject to unauthorized access, alteration, destruction or disclosure.
- **Sensitivity**: Processing certain categories of especially sensitive data is subject to a stricter control than other personal data.

Thus, a privacy policy may be legally assessed under legislation that implements these principles. For example, if a particular policy does not provide for a fair processing, then the rules included in the policy may be void. Nevertheless, for most people it is challenging to assess whether they should consent to the processing of their personal data under a given privacy policy, particularly if it is ambiguous and permits a wide range of forms of processing personal data, possibly exceeding what would be permitted under the applicable data protection law. For the data subject it often remains unclear to what, exactly, she is consenting and for what purposes and by whom the data will be processed. This reflects the vast economic imbalance between the data subjects and the data controllers.

All of these factors make the practical protection of personal information rather challenging. The approach outlined in the remainder of this paper might, if successful, solve some of these shortcomings.

3 An Infrastructure for Privacy Policy Referencing

The fundamental principle of Privacy Policy Referencing is that all personal information must be tagged or associated with metadata that relates it to the applicable privacy policy, and possibly to the point and time of collection. This would enable users or authorities to audit systems and applications where personal information is being processed, and to determine whether they adhere to applicable privacy policies. By making it mandatory to always have policy metadata associated with personal information, it becomes a universal principle for referencing privacy policies. In other words, a pointer to the relevant privacy policy will always follow the data. The PRIME FP7 research project[6] developed concepts based on HP Labs 'Sticky Policies' approach, where personal data is stored and communicated in encrypted data containers with attached policies [5].Their approach, however, assumes that the underlying hardware platform, and the software running on it, are so-called trustworthy systems based on the Trusted Computing specification. To improve personal data processing in reality, all information systems that can get a hold of data must be based on such platforms. However, a complete market penetration is not realistic in the near future. Recently, concepts such as 'Obligations Management' and 'Audit Trails' have come into focus of the FP7 PRIMELife project[7], which shall provide organizational and technical awareness and auditability of personal data handling in corporate and large IT systems [2]. This will not put any extra burden on the users, but will require the establishment of totally new frameworks for organizations, which can be grouped into technical, policy, management and legal frameworks. These will be discussed below.

3.1 The Technical Framework

Privacy policy metadata will require the definition of a common metadata language in XML style. A conceptual visualization of personal information with associated privacy policy metadata is illustrated in Fig.1 below.

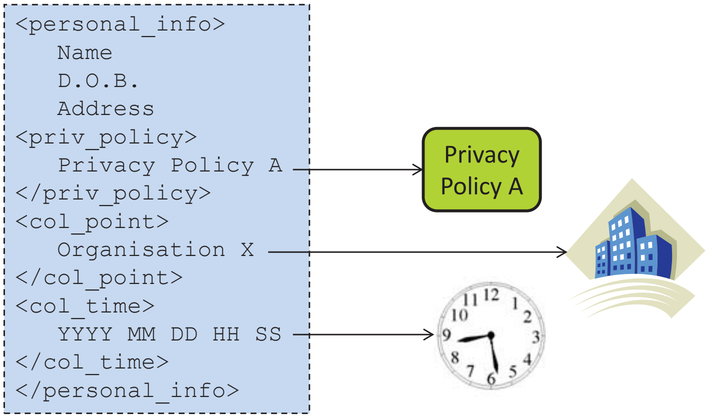
Typical tags that need to be defined are the privacy policy identifier, date of collection, and type of consent given by the user. This means that each privacy policy must be uniquely identifiable, so that organizations must keep records of such identifiable privacy policies that have been used. The integrity of the policies can be ensured, e.g. with cryptographic means. The metadata does not need to contain any additional personal information, because that would be irrelevant for potential audits of policy adherence.

There are situations where it is impractical to have the metadata stored directly together with the personal information, e.g. when personal information is being processed with very high speed and high volume. The organizations must then find a solution for associating the personal information with metadata stored elsewhere.

It can be noted that our scheme has similarities with the scheme for electronic signature policies described in [25] where a specific signature policy has a globally unique reference which is bound to the signature by the signer as part of the signature calculation. This thereby provides non-repudiation for the applicable signature.

[6] see http://www.prime-project.eu

[7] see http://www.primelife.eu/



```
<personal_info>
   Name
   D.O.B.
   Address
<priv_policy>
   Privacy Policy A
</priv_policy>
<col_point>
   Organisation X
</col_point>
<col_time>
   YYYY MM DD HH SS
</col_time>
</personal_info>
```

Fig. 1. Personal information with associated privacy policy metadata

3.2 The Policy Framework

It is very difficult for users to understand privacy policies when each organization specifies a different policy and when typical policies are 10 pages or more. In order to increase the usability and accessibility of privacy policies, a set of standard privacy rules and policy profiles can be defined. Let a specific privacy rule be denoted as P-Rule n where n is a number. Then a set of compatible and coherent rules will constitute a specific profile denoted as PR-Profile X where X is a letter. The combination of rules into specific profiles can be denoted as the PRP (Privacy Rules Profile) framework. The purpose of defining PR-Profiles is that a specific privacy policy can simply be defined and expressed as a PR-Profile within this framework. The PRP framework is illustrated in Fig.2

It is also possible to have more of less strict versions of each profile, so that a profile e.g. can be called ”PRP-B level II”, where ”level II” indicates options within the specified profile. To some degree, elements of privacy policies could be standardized at least at a national or regional level, for example under the auspices of the Article 29 Working Party of the EU. Ideally, a standardization on an international level would also be desirable, so that it is possible to define meaningful policies that could be interpreted in a global context. However, this would be challenging, as such policies would have to be assessed under the different national legal frameworks of data protection laws.

In this respect, one might benefit from the experiences of standardizing other contract clauses. For example, in international trade law, the Incoterms [17] offer a widely used catalogue of specific contract terms that can be quoted when buying or selling goods. One of the advantages of the Incoterms are that they address very specific issues, enabling contract parties to simply reference a brief abbreviation (e.g. FCA) to agree on a number of basic terms. Characteristic for the Incoterms is, however, that they do not include a comprehensive set of rules for a contract, which is described in a lengthy contract text. This distinguishes this type of contract standardization from another ex-

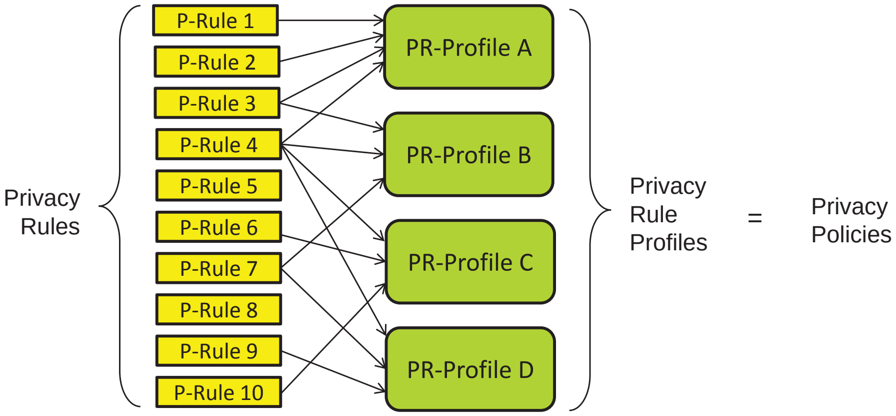


Fig. 2. The Privacy Rules Profile Framework

ample, which is arguably more well-known in the IT community. A number of IPR licensing issues regarding open source software can be easily regulated by referring to specific predefined licenses. For example, the Open Source Initiative publishes a list of approved licenses (http://opensource.org/licenses/alphabetical). In data protection law, contractual frameworks have been standardized, for example, in order to regulate the transfer of personal data to countries outside the EU legal framework [12].

Instead of specifying a lengthy policy, organizations could simply refer to a standardized policy profile that is specified elsewhere. By having limited set of standardized policies, it would be possible for users to become educated and familiar with what the respective policies actually mean, and the level of protection they provide. Assuming that users are familiar with privacy policies A, B, C and D in terms of their PRP (privacy rules profiles), a reference to e.g. Policy-B will be meaningful for users, without having to read several pages of text. Moreover, the recommendation of some trusted entity of certain policies could be informative for those users not wanting to read the whole policy themselves.

3.3 The Management Framework

Organizations would need to manage their privacy policies according to strict criteria, and define a way guaranteeing their integrity and authenticity. This can e.g. be achieved by letting independent third parties sign hashes of each particular policy or policy profile which would allow changes in policies or profiles to be noticed, or to deposit the privacy policies with independent third parties such as national information commissioners and data protection inspectorates. Privacy policy repositories that are suitable for long-term archival of verified policies might me necessary with respect to long-term legal validity. Organizations will also need to define processes for creating metadata and to adapt applications where personal information is being processed so that the metadata can be appropriately handled during storage, transfer and processing.

3.4 The Legal Framework

This approach could also be complemented with respective changes to the legal framework as e.g. through [24], in order to provide incentives for its adoption. Otherwise, data controllers might not be interested in this approach, as it may ultimately limit their possibilities of processing personal data.

For example, it could be considered to oblige certain data controllers – particularly those collecting vast amounts of personal data – to associate valid privacy policy metadata to all personal data. This could be seen as an extension of the purpose specification principle mentioned above, according to which personal data can only be collected for specified, explicit and legitimate purposes and not further processed for other purposes. An additional element might be that that certain classes of privacy policies could be mandatorily deposited with a respective national or regional data protection authority, and that the metadata points to the deposited copies of the privacy policies, who might also assess a policy's compliance with the applicable law. This might enhance the possibilities for auditors to review data controllers with regard to the personal information that that they process. Assume that the privacy policy referred to by the metadata specifies that the personal information shall not be transferred to third parties, and that the metadata also indicates a specific organization's web interface as the point of collection as well as the time of user consent. In case the audited organization is different from the organization specified in the metadata, the auditor will have an indication that the privacy policy has been infringed.

4 Conclusion

The current approach to ensuring personal information privacy on the Internet is ineffective in providing privacy protection in the age of distributed, networked services. In this paper, we have argued that the traditional method of accepting privacy policies by ticking boxes provides very poor user understanding, and hence poor consent as required by the law.

The approach described in this paper changes the way privacy policies can be specified by service providers, and compliance be verified by auditors or users. By providing certified template policies, users gain oversight of policies that have been verified. At the same time, auditors can verify system states against policy claims. Finally, based on using metadata as a pointer to applicable privacy policies, and by use of specifying policies as standardized profiles, a connection between data, user, consent and policy is maintained. Introducing this framework might also require the introduction of incentives, for example by making it mandatory to include privacy policy metadata with personal information. Remaining challenges, such as the international synchronization of policy templates, the reliable, auditable and secure implementation of personal data handling with policies, and the creation of the default policies and their supervision and archival, need to be further researched.

References

1. Annie I. Antón, Julia B. Earp, and Angela Reese. Analyzing Website Privacy Requirements Using a Privacy Goal Taxonomy. In IEEE Computer Society, editor, *Proceedings of the IEEE Joint International Requirements Engineering Conference 2002*, pages 605–612. IEEE Computer Society, Essen, Sep. 9-13, 2002 2002.
2. C.A. Ardagna, L. Bussard, S. De Capitani di Vimercati, G. Neven, E. Pedrini, S. Paraboschi, F. Preiss, P. Samarati, S. Trabelsi, and M. Verdicchio. Primelife policy language, November 2009.
3. Lee A. Bygrave. Data Protection Law, Approaching its Rationale, Logic and Limits. In *INFORMATION LAW SERIES Volume 10*, pages 57–68. Kluwer Law International, 2002.
4. P. Carey. *Data protection: a practical guide to UK and EU law*. Oxford University Press, 2004.
5. Marco Casassa Mont, Siani Pearson, and Pete Bramhall. Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services. In *Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03)*, page 377. IEEE Computer Society, 2003.
6. A. Cavoukian and M. Crompton. Web Seals: A Review of Online Privacy Programs. A Joint Project of The Office of the Information and Privacy Commissioner/Ontario and The Office of the Federal Privacy Commissioner of Australia, http://www.ipc.on.ca/english/pubpres/papers/seals.pdf, Venice, September 2000.
7. European Comission. 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). Technical report, July 12, 2002 2002.
8. L. Cranor et al. *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*. W3C Recommendation 16 April 2002, http://www.w3.org/TR/P3P/, 2002.
9. Claudia Diaz. Profiling Game. January 2005.
10. Claudia Diaz and Bart Preneel. Anonymous communication. In Swedish Institute of computer science, editor, *WHOLES - A Multiple View of Individual Privacy in a Networked World*, Stockholm, 30-Jan-2004 2004.
11. P. Dutton. Trust Issues in E-Commerce. In *Proceedings of the 6th Australasian Women in Computing Workshop*, pages 15–26. Griffith University, Brisbane, July 2000.
12. EC. STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES, Commission Decision 2004/915/EC of 27 December 2004. In *Official Journal L 385 of 29.12.2004*. European Commission, 2004.
13. European Council. 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., 23rd November 1995.
14. Lothar Fritsch. Profiling and location-based services. In M. Hildebrandt and S. Gutwirth, editors, *Profiling the European Citizen - Cross-Disciplinary Perspectives*, page 147160, Dordrecht, April 2008.
15. Lothar Fritsch and Habtamu Abie. A Road Map to the Management of Privacy Risks in Information Systems. In Gesellschaft f. Informatik (GI), editor, *Konferenzband Sicherheit 2008, Lecture Notes in Informatics LNI 128*, volume 128 of *Lecture Notes in Informatics (LNI)*, pages 1–15. Gesellschaft für Informatik, Bonn, April 2008.
16. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein. *Datenschutz-Gütesiegel*. 2003.
17. ICC. *Incoterms 2000: ICC Official Rules for the Interpretation of Trade Terms. ICC Publication No.560, 2000 Edition*. 2000.

18. Claudia Koch. *Taxonomie von Location Based Services - Ein interdisziplinärer Ansatz mit Boundary Objects*. PhD thesis, Johann Wolfgang Goethe - Universität, Frankfurt am Main, 2006.
19. Oleksiy Mazhelis and Seppo Puuronen. Combining One-Class Classifiers for Mobile-User Substitution Detection. In *Proceedings of 6th International Conference on Enterprise Information Systems (ICEIS'04)*, pages 130–137. Porto, 2004.
20. M. Mithal. Illustrating B2C Complaints in the Online Environment. Presentation by the US Federal Trade Commission and Industry Canada, at the Joint Conference of the OECD, HCOPIL, ICC: Building Trust in the Online Environment: Business to Consumer Dispute Resolution (The Hague), December 2000.
21. OECD - Organisation for Economice Co-Operation and Development. Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data., 23rd September 1980.
22. The Treasury Board of Canada. *Privacy Impact Assessment Guidelines Version 2.0 - A Framework to Manage Privacy Risks*. August 2002.
23. Andreas Pfitzmann and Marit Köhntopp. Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology . In Hannes Federrath, editor, *Designing Privacy Enhancing Technologies*, volume 2009 of *LNCS*, pages 1–9. Springer Verlag, Heidelberg, 2001.
24. Viviane Reding. *Privacy: the challenges ahead for the European Union* (Keynote speech at the Data Proteciton Day), SPEECH/10/16. 28 January 2010. European Parliament, Brussels. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/16, 2010.
25. J. Ross, D. Pinkas, and Pope. N. *RFC 3125 - Electronic Signature Policies*. IETF, September 2001. Available at: http://www.rfc-editor.org/.
26. Daniel Solove. A taxonomy of privacy - GWU Law School Public Law Research Paper No.129. *University of Pennsylvania Law Review*, 154(3):477, Jan. 2006 2006.
27. Sandra Steinbrecher and Stefan Köpsell. Modelling Unlinkability. In Roger Dingledine, editor, *Proceedings of Privacy Enhancing Technologies workshop (PET 2003)*, volume 2760 of *LNCS*. Springer Verlag, 2003.
28. Cooperation Group Audit Strategy. Privacy Audit Framework under the new Dutch Data Protection Act (WBP). Technical report, Den Haag, 2001.
29. The Economist. The Coming Backlash in Privacy. *The Economist Technology Quarterly*, 2000. December 9.
30. Tony Vila, Rachel Greenstadt, and David Molnar. Why we cant be bothered to read privacy policies: models of privacy economics as a lemons market. In *Proceedings of the 5th international conference on Electronic commerce (ICEC03)*, page 403407. ACM Press, Pittsburgh 2003.