Journal of Information, Law and Technology

Laws, PETs and Other Technologies for Privacy Protection

John J. Borking, Vice President,
Dutch Data Protection Authority (Registratiekamer)
Email: *jbo@registratiekamer.nl*

Charles D. Raab, Professor of Government,
University of Edinburgh
Email: *c.d.raab@ed.ac.uk*

This is a **refereed** article published on: 28 February 2001

Citation: Borking J and Raab C, 'Laws, PETs and Other Technologies for Privacy Protection' Refereed Article, 2001 (1) *The Journal of Information, Law and Technology (JILT)*. <http://elj.warwick.ac.uk/jilt/01-1/borking.html>

Abstract

This article explains Privacy-Enhancing Technologies (PETs), their anchoring in the Dutch Personal Data Protection Act (WBP) and other data-protection systems, and how they might contribute to the lawful processing of personal data.

Keywords: Privacy; Data Protection Law (Netherlands), Privacy-enhancing Technologies, (PETs), Privacy-Incorporated Software Agent (PISA), Identity Protector.

1. Introduction

The application of information and communications technologies (ICT) for the sake of privacy protection has become widely known under the name of Privacy Enhancing Technologies (PETs). PETs have been defined as a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system. PETs have already achieved an important place in the practical and theoretical repertoire of privacy-protection instruments in most, if not all, countries where data-protection laws and systems are already in place or are being created. It is therefore relevant to clarify and explain the role that PETs may be expected to play in the safeguarding of personal data and of privacy· Although this article is based mainly on a consideration of developments in the Netherlands, it has a broader significance in view of the global nature of personal-data activities and the similarity of problems faced by countries aiming to protect privacy by means of systems of data protection.

2. The Basic Level and Principles of Privacy Protection

The introduction of the Personal Data Protection Act (*Wet bescherming persoonsgegevens*/WBP) in the Netherlands in 2001 in accordance with the European Data Protection Directive 95/46 of 1995 involves consequences for all organisations in the public and private sectors. The Act covers computerised and non-computerised data processing, requiring that the parties involved in data processing ensure that WBP rules are correctly followed. This involves a directed approach to the activities that must be undertaken in the context of the act. It is expected that previous measures and procedures with regard to control, security and processing be reconsidered and possibly revised and tested against the current WBP objectives. When asked about the measures they have taken to protect privacy, organisations will usually claim that they have invested their best efforts to secure personal data. Although the use of security measures to prevent unauthorised access to personal data is a significant component of privacy protection, such security cannot efficiently protect privacy. It must be clear that more needs to be done to protect privacy technologically, including the application of PETs. The EU directive 95/46 and consequently the national privacy legislation based on it thus have consequences for system developers·

As the reply of the Minister of Justice to Dutch Parliament's First Chamber regarding

WBP states, current ICT could be a significant aid in making sure that processing activities handle personal data in a correct and careful manner. In many countries, the framework of data protection law and practice within which PETs take their place consists of legislated regulations concerning the processing of personal data. The WBP, for instance, sets forward a number of rules and principles governing lawful processing. These generally conform to the conventional privacy principles and guidelines that are found in national privacy laws and in international instruments such as the Council of Europe Convention, the OECD Guidelines, and the EU Directive. The WBP rules concern the following:

1. *Reporting the processing*
   The processing of personal data must be reported in advance to the Data Protection Board or a privacy officer, unless processing has been exempted.

2. *Transparent processing*
   The person involved must be able to see who is processing his personal data and for what purpose.

3. *'As required' processing*
   Personal data may only be collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

4. *Lawful basis for the data processing*
   The processing of personal data must be based on a foundation referred to in the WBP, such as permission, agreement, legal obligation, justified interest and such like. For special data, such as health, stricter limits prevail.

5. *Data quality*
   The personal data must be as correct and as accurate as possible, sufficient, to-the-point and not excessive.

6. *Rights of parties involved*
   The parties involved have the right to take cognisance of and to improve their data as well as the right to raise objections.

7. *Data traffic with countries outside the EU*
   In principle, the traffic of personal data to a country outside the EU is permitted only if that country offers adequate protection.

8. *Processing personal data by a processor*
   If processing is outsourced to a processor, it must be ensured that he will observe the instructions of the person responsible.

9. *Protection against loss and unlawful processing of personal data*
   Suitable measures of technical and organisational nature make up the necessary tailpiece of lawful processing.

The requirements referred to in the WBP must be implemented efficiently in the organisation in order to give proper support to the citizen's right to privacy with respect to personal data. It is therefore important to devise a proper system of general processing measures and procedures that should be present in order to protect company processes and in connection with specific protective measures for the processing of personal data. The restrictions that the organisation of data systems can impose on the possibility that their users can comply with privacy legislation are evident. One simple example is where a system contains an inescapable 'date of birth' field, while analysis of the company's processes shows that recording the birth date of all persons included in the system is excessive. System design can just as easily ensure that users correctly observe the law. As a rule, privacy protection will constitute a supplementary system of measures and procedures in addition to the usual processing and security measures, but it should be assigned a significant place in management processes in order to implement and maintain a balanced processing policy for personal data.

3. The Legal Context for PET Development

The EU Directive 95/46 provided the sharpest stimulus for the revision of data protection legislation in the Member States from the late 1990s on. The incorporation of PETs into strategies for privacy receives some encouragement from Article 17 of the Directive, which requires data controllers to implement 'appropriate technical and organisational measures' to protect personal data, especially in network transmissions. Recital 46, which augments the meaning of Article 17, highlights the requirement that these measures should be taken 'both at the time of the design of the processing system and at the time of the processing itself', thus indicating that security cannot simply be bolted onto data systems, but must be built into them. This provision mainly concerns data security, but it is generally intended as a safeguard against other forms of unlawful processing. This has been transposed into Dutch law as Article 13 of the WBP:

> 'The person responsible shall ensure suitable technical and organisational measures to protect personal data against loss or any form of unlawful processing. Taking into account the technical status and enforcement expenses, these measures shall guarantee suitable protection given the risks that accompany the processing and the nature of the data to be protected. The measures should also avoid unnecessary collection and the further processing of personal data'.

During considerations in the Second Chamber, the last sentence of Article 13 was added by Second Chamber members Scheltema-de Nie and Wagenaar by means of amendment 22. Discussing the Dutch Privacy Protection Act in the Upper House, the Minister of Justice said that:

> 'current IT capabilities to abuse personal data necessitate a search for supplementary possibilities to make sure personal data are treated properly and accurately. Consider partial or complete 'anonymising', for instance, by eliminating from personal data their identifying characteristics, or protecting them against use by certain applications/users, or by limiting their use to certain

> purposes. In this thinking, amendment 22 of the Lower House to Article 13 of the bill added that the prescribed security measures must also focus on the prevention of unnecessary collection and further processing of personal data. This will provide a legal foundation for the application of PETs. Such rules respond to the restrictions of the developing information technology'.

Article 13 thus outlines that the person responsible for the processing of personal data takes suitable technical measures to protect personal data. Wherever technical measures are insufficient or unfeasible, organisational measures can be taken, or organisational measures can enhance the technical measures in a coherent package. Whenever there is a choice between organisational and technical facilities as part of a balanced processing policy, the Data Protection Board always prefers the latter. Technical measures are usually more efficient, as it is more difficult to escape their effects. While the definition of 'organisational measures' is left open, it is important to note that it draws attention to managerial and other human systems through which technical devices are put into effect, and therefore opens up a path towards shaping the regimes of staff accountability and responsibility within business firms or government agencies.

A further legislative provision is that the Lower House accepted Motion 31 of member Nicolaï, in which the government is enjoined to apply such technologies to its own data systems. The explanatory memorandum of the Ministry of Home Affairs for 2001 indicates that NLG 10-15 million will be necessary each year to enforce the 'Contract with the Future' memorandum to give the government's role real meaning as a booster and user of technological innovation, including PETs. In its letter of 13 January 1999, the Data Protection Authority (Registratiekamer) pointed out to the Lower House that:

> 'this means that the person responsible will have to take suitable measures against collecting, recording and saving personal data in violation of the conditions set elsewhere in the WBP. In particular this means that collecting and processing personal data without sufficient basis as referred to in Article 8 of the WBP will have to be prevented. Article 13 of the WBP makes the person responsible translate the legal standards of the WBP into the actual processing of personal data and also take this into account when designing and further developing data systems'.

4. The PET Report

In keeping with data protection principles and their practical application to particular personal data systems, research and development towards the establishment of PETs as a leading set of instruments for privacy protection led to the publication, in August 1995, of the report *Privacy Enhancing Technologies - the Path to Anonymity*, written in association with TNO/FEL (the Dutch national research centre) and the Information and Privacy Commission of Ontario, Canada. There has been five years of experience in the Registratiekamer with this, and research continues towards its realisation in practice. The report's researchers posed two central questions:

- what conditions must be kept in mind when engineering an information system in order to guarantee that the system be used effectively and efficiently without revealing the user's identity?

- what types of information and communication technology can contribute towards achieving this goal?

The main issue that was also posed was whether identity is necessary for all processing steps within a data system. The report shows that in many cases the identity of the user, consumer or citizen is irrelevant. In some cases, however, identity *is* relevant for legal reasons, for instance to pay for certain services, or to open a bank account.

To implement matters technically, a system element called the 'identity protector is used within the data system to convert the identity of the person involved (the person whose data are being processed - the 'data subject') into one or more pseudo-identities. The placement of the identity protector provides for at least two different domains within the data system; one domain where the identity of the person involved is known or accessible (the identity domain) and at least one domain where this is not the case (the pseudo-identity domain). The aim of the pseudo-identity domain is to make sure the person involved cannot be traced on the basis of previously obtained personal data, and vice-versa, to make sure the personal data cannot be found on the basis of the obtained identity.

The identity protector in a data system can take several forms, for example:

- a separate function implemented in the data system;

- a separate data system supervised by the individual (for instance, the smart card for biometrics identification);

- a data system supervised by a party entrusted by a service provider and consumer ('Trusted Third Party' (TTP)).

The use of an identity protector thus makes it possible to intervene preventively within the data system to hide the identity of the person involved. Other possible techniques are digital signatures, blind digital signatures, digital pseudonyms, digital certificates and MIX nodes.

5. PET Strategies: Identification and the Criterion of Disproportionate Effort

In applying PETs, the person responsible can choose two strategies: either focusing on preventing or reducing identification; or focusing on preventing unlawful processing of personal data, in accordance with the WBP. A combination of both is also possible.

As to the first option, PETs involve consequences for personal data within data systems.

To determine this, it must be clear what personal data are. In legal terms, personal data means any piece of information regarding an identified or identifiable natural person. Whether we can talk of ‘personal data’ depends on a number of elements of which, within the scope of this document, ‘identification’ is the only significant element. According to Article 2 of the EC Directive 95/46, a natural person can be identified ‘directly or indirectly’. Direct identification requires basic details (e.g., name, address, etc.), plus a personal number, a widely known pseudo-identity, a biometric characteristic such as a fingerprint, etc. Indirect identification requires other unique characteristics or attributes or a combination of both, to provide for sufficiently identifying information. PETs make it possible to render anonymous or to ‘anonymise’ the directly identifying data. Once data have also been emptied of indirectly identifying characteristics, then one can speak of a situation in which there are no personal data and the protective stipulations of the Directive and the WBP are no longer applicable.

Non-identification is also assumed if the amount and the nature of the indirectly identifying data are such that identification of the individual is only possible with the application of disproportionate effort, or if assistance by a third party outside the power and authority of the person responsible is necessary.Whether we can talk of disproportionate effort depends, on the one hand, on the nature of the data and the size of the population; and on the other hand, the resources of time and money one is willing to spend in order to be able to identify the person.

6. PET Strategies: Securing Against Unnecessary Processing

PETs can also be applied for protection against various forms of unlawful processing of personal data, including unlawful kinds of collection, recording, storing, disclosure (within or between organistions), and matching or sharing. In implementing PETs in these aspects of processing, the person responsible can choose to structure his or her data system using identity and pseudo-identity domains, so that fewer or no personal data are being processed (for instance when collecting or recording) and/or, depending on the protocols within the data system, provision of or access to anonymised data are or are not allowed for various users. For scientific research and statistical processing, for instance, access to non-identifying data may be granted, whereas in hospitals, identifying data can be provided on the basis of functional authorisation and the relationship between care-provider and patient. Further, when testing data processing against the privacy principle of fair and lawful processing, PETs can fulfil a significant role; that is, if the test indicates that certain data may not be processed or that only strictly necessary data may be processed. If the ‘as required’ character has been determined normatively and PETs are applied within the scope of lawful justification, PETs can also contribute to the retention of the ‘as required’ stipulation.

Finally, PETs can easily be applied within the scope of protection against unnecessary and/or undesired processing. This is in accordance with the clarification of Article 13 of WBP and Article 17 of the EU Directive 95/46, in which it is pointed out that this Article covers all parts of data processing. An example is relevant here: in June 1997, an international software house developed and successfully marketed a PET-enabled hospital information system to hide the true identity of the patient and the carer as well as the related information in the database. Pseudo identities are used here by means of the identity protector to ensure that the person's identity cannot be established from related data in the database, and that the related data cannot be revealed once a person is identified. In the Client/Server architecture of this system, the required relations in the database have been removed and all information is encrypted. The identity protector manages access to the required information. A typical dialogue in this PET database is as follows:

- log in with name of physician;
- check in table 'physician';
- return sequence primary key of physician;
- encrypt to pseudo identity ('pid') of physician;
- search table 'care relation';
- return sequence primary key of patient(s);
- search table 'patient';
- select patient;
- encrypt to 'pid' of patient;
- search table 'appointment' with 'pid' of physician and 'pid' of patient;
- return appointment(s);
- etc.

Nobody without a functional authorisation in this PET system can process any data in it. Even if privacy protection is not at stake, using PETs provides for significant data security. The effect of PETs on the performance of the database has been tested in the hospital information system described above. The performance in efficacy and response time was not affected by the application of PETs functionalities. The costs for building in these functionalities was 1 percent more than without, due to the fact that PETs functionalities have been incorporated into the design (data model) from the beginning.

Whether, in all reasonableness, PETs can be required depends on all the weighted factors in the situation, as the Registratiekamer's letter of 13 January explained by referring to the criteria laid down in article 13 of the WBP, concerning technical status, cost and risk. As the realisation of increasing effectiveness becomes possible through PETs, a suitable protection level as referred to in Article 13 will in increasing numbers of cases be impossible without PETs. PET opportunities will increase if measurable and quantifiable experience increases show that PETs offer efficiency advantages for data processing policy, for instance by simplifying procedures, avoiding red tape through better business processes, or reinforcing security. However, the application of PETs in old, existing data systems is not always feasible. For example, opening up existing data systems to introduce an identity protector can be very expensive. In addition, the owner of the old data system often lacks the courage and will to carry out such operations as the 'spaghetti' often cannot be disentangled due to the many releases and patches.

The major opportunities for PETs are therefore in the design and implementation of new data systems. The latest data systems often do not completely comply with the requirements set in the Personal Data Protection Act or the related legislation. To implement efficiently the requirements formulated in the WBP, it is important to realise a proper system of general processing measures and procedures on the basis of the protection of company processes and in connection with specific protective measures for the processing of personal data. It has already been indicated that PETs offer an excellent means to be applied effectively to enhance a balanced policy for the processing of personal data. Organisational measures will remain necessary besides the preventive technical measures provided by PETs, although on grounds of reliability there are many reasons why PETs may be preferred.

How can the quality of PETs be vouched for in specific applications? Societies show an increasing demand for prompt and unequivocal insight into product quality and services, and PETs similarly may be required to prove themselves. Such quality statements are frequently expressed via a certification issued by an expert or independent third party. Such certification can play a significant role in clarifying whether PETs have been applied effectively to a data system. To issue such certification a 'PET scan' might take place according to a pre-determined certification procedure. These certifications would indicate that the data system concerned has been built in such a way that it can be stated with reasonable certainty that with the help of PETs, the intended protection of personal data has been properly provided. This technique bears some resemblance to privacy impact assessments, which are receiveing attention in many countries as part of the armoury of data protection. Computer science researchers are trying to measure the level of privacy provided - computational, information-theoretic and perfect-forward anonymity - by various systems. Perhaps we will see in five years time the use of an 'identity protector meter' giving the user feedback about his or her current level of protection by, for example, indicating that the anonymity level is low in high network traffic, with the warning that the privacy risk to be observed is very high.

This means that introducing PETs into systems is not only a technical job, but also a normative and evaluative one. In the Netherlands, before PETs are 'INSIDE' data systems, it must be clear what requirements the WBP sets on a data system. This directly affects the exercise of the tasks of the Data Protection Authority in its entirety. As long as it is not clear what standards the data processing needs to comply with in a specific situation, the term 'PET-INSIDE' will remain meaningless. Technologists and jurists will need to translate legal requirements into technical system specifications and, vice versa, use a PET scan to test whether system requirements and applications comply with the

WBP. However, much more time and effort has to be reserved for this work within the Data Protection Authority than is available today if timely, proactive privacy protection will be available for the citizen in the future.

The available arsenal of PET systems within networks is becoming ever larger, enabling non-identification of user and provider, as well as ensuring the invisibility of the network, server, query, etc. In practice, PET systems are being developed at many places (e.g., the Research University of Dresden, ICSI in Berkeley, CA, and TNO/FEL) or are being introduced commercially onto the market using an identity protector or similar techniques. Yet it is estimated that in the Netherlands fewer than 0.1 percent of data systems are currently using PETs. The introduction of the WBP, the enforcement of the Nicolaï motion mentioned above, and the increasing autonomous demand for better data security and protection of information privacy is likely to change this over the coming years.

7. Other Privacy-supporting Technologies

Due to the limitations on the implementation of PETs discussed above, the most frequent path for organising data systems is likely to be one whereby the person responsible combines PETs and other privacy advancing technologies is expected to be applied most frequently. There are many other technologies that might also contribute to better privacy protection if PETs (with Identity Protector and domains) cannot be applied effectively. This is certainly the case with the following data processing conditions derived from basic privacy principles: transparency, data quality, respect for the rights of parties involved, and security.

For example, transparency might be advanced by means of P3P (a technique to test websites' privacy policy), yet this depends mainly on the default setting. This should be so structured that not all data entered can be accessed automatically. The rights of the parties involved can be better safeguarded by means of feedback and control. The design principles should ensure that the individual may check at any desired moment regarding what personal data he/she has given to the data systems, with the possibility to peruse, supplement, alter and delete personal data. In media spaces (computer-controlled networks of audio-video equipment and digital networks used to support communication and collaboration amongst people within a group separated by architecture in a building or by geographical distances through nodes), where a moment-to-moment continuous control is used, researchers found that people felt uneasy about their lack of ability to monitor and control their self-presentation and consequently their privacy. Control empowers people to stipulate the information they project and who can get hold of it, while feedback informs people when and what information about them is being captured, and to whom it is being made available. The more interaction is required, the more reciprocity (if I can see you, you can see me) needs to built into the system.

As for security, collecting and recording the origin of the data can be logged automatically. Automatic logging is also possible when retrieving, consulting, altering or supplying data within the organisation or to another one. Such log-ins should be deleted with the help of the system administrator, whereby such deletion is turned into a log for which the person responsible will have to account. The same applies to access control: automatic access control is used as a means of security in protecting, consulting, altering, deleting and destroying data. It is also possible to apply automatic data deletion. Storage time can be determined by the software; data are deleted automatically once the storage time elapses. As to processing by a processor who is not the data controller, and the flow of data outside the EU, technical measures can be adopted to prevent unlawful actions in terms of the WBP. Many data systems have the functionality to detect the IP address while automatically analysing who is visiting a web site. While processing this information, Some systems run tables in which all IP addresses are stored, enabling them to find the country and the language used by the sender, and immediately presenting the required information on the web site in that language. The same technique can, by analogy, be used while sending electronically information to a country outside the EU. For example, an e-mail address outside the EU will be detected and the transmission of data will be stopped, provided this functionality is embedded in the data system.

From the range of possibilities, the person responsible can choose PETs only, or other privacy advancing technologies, or a combination of both. The aim of these measures is important in all cases. If only one of the WBP-determined basic privacy standards is achieved through technological means, that technology in itself is not sufficient to realise optimal privacy protection. For instance, a statistical linguistic analysis application within an address system can fully optimise data correctness, yet it cannot guarantee privacy protection in a wider sense. In contrast to such a singular technique, a multiple technique would be to combine a number of stacked technical measures at the same time within the data system; for instance, distributed storage with origin protocolling, the use and supply of data, etc. This might lead to a satisfactory privacy-secure environment. Although theoretically, current ICT applications can implement at least one privacy principle in any data system, it is sometimes so prohibitively expensive in proportion to the interest to be protected that introducing such technical measures cannot be justified. Therefore, if neither PETs nor any other technical measure can be introduced, then procedural measures will need to be applied to guarantee the privacy of the consumer or citizen whose personal data are stored. A *caveat* that needs to be entered with any technologically-based privacy solution is that it may be effective only as long as users stay within the PET-enabled information system. Once the authorised user exports the decrypted data to another environment, for example by printing them on paper or transferring them to a different medium or to a secondary user, the chain of PETs protection is broken. Better privacy protection may depend upon the existence of a more comprehensive regime that includes other forms of safeguards, operating through laws or effective codes of practice, as a context within which PETs may play a part.

8. Conclusion

Developments in ICT are providing ever more possibilities to collect, store, process and distribute personal data. The potential violations of consumer and citizen privacy increase consequentially. However, that very same ICT offers solutions in the shape of privacy protection for user, consumer and citizen. PETs are a promising aid to achieve basic privacy norms in lawful data processing. Of course, attention and research will remain necessary for PETs, and the Data Protection Authorities will need to continue to invest best efforts to stimulate PET applications in data systems, such as is the case in the current PISA project. PETs are being encouraged in other countries as well, as part of a comprehensive and systematic approach to privacy protection that accords a significant role to technological means of protection without assuming that they are a 'magic bullet' that can be aimed at the target without the accompaniment of legal, organisational, ethical and educational tools. It will also need to be checked, via privacy auditing or specific PET scans, whether PET-equipped systems indeed comply with privacy legislation. Certification within the scope of a privacy audit might contribute to this and offer the necessary certainty to the citizen and consumer that the privacy of his or her personal data is being effectively protected.

References

Bellotti, V. and Sellen, A., *Design for Privacy in Ubiquitous Environments,* Cambridge (UK): Rank Xerox EuroParc, 1993.

Berthold, O., Federrath, H. and Kopsell, S., 'WebMIXes: A System for Anonymous and Unobservable Internet Access', in *Proceedings of the Workshop on Design Issues in Anonymity and Unobservability*, Berkeley (CA), 2000, pp.101-115.

Berthold, O., Pfitzman, A. and Standtke, R., 'The Disadvantages of Free MIX Routes and How to Overcome Them', in *Proceedings of the Workshop on Design Issues in Anonymity and Unobservability*, Berkeley (CA), 2000, pp. 27-42.

Blarkom, G. van, *Security of Personal Data of the Dutch Data Protection Board*, A&V Study No. 23, The Hague, 2001.

Borking, J., 'Der Identity Protector', *Datenschutz und Datensicherheit*, 11, 1996, pp. 654-658.

Borking, J., 'Einsatz datenschutzfreundlicher technologien in der Praxis', *Datenschutz und Datensicherheit*, 11, 1998, pp. 636-640.

Borking, J., 'Health Cards, Protection or Intrusion of Privacy?, in Broek, L. van der and Sikkel, A. (eds.), *Health Cards '97: Studies in Health Technology and Informatics*, Vol. 49, p. 162, Amsterdam 1997.

Borking, J., 'Privacy Protecting Measures in IT Environment Necessary', *Information Management*, 10, 1998, pp. 6-11.

Catlett, J., 'Open Letter to P3P Developers & Replies', in *CFP2000: Challenging the Assumptions, Proceedings of the Tenth Conference on Computers, Freedom & Privacy*, New York: Association for Computing Machinery, 2000, pp. 155-164 (also available at <http://www.junkbusters.com/ht/en/standards.html>).

Lessig, L., *Code and Other Laws of Cyberspace*, New York: Basic Books, 1999.

Clarke, R., 'Identification, Anonymity and Pseudonymity in Consumer Transactions: A Vital Systems Design and Public Policy Issue', in *Conference on 'Smart Cards: The Issues'*, Sydney, 18 October 1996, available at <http://www.anu.edu.au/people/Roger.Clarke/DV/AnonPsPol.html>.

Cranor, L., 'Privacy Tools', in H. Bäumler (ed.), *E-Privacy: Datenschutz im Internet*, Braunschweig: Vieweg, 2000, pp. 107-119.

Datenschutz und Datensicherheit, 7, 1997, Schwerpunktheft 'Digitales geld'.

Dingledine, R., Freedman, M. and Molnar, D., 'The Free Haven Project - Distributed Anonymous Storage Service', in *Proceedings of the Workshop on Design Issues in Anonymity and Unobservability*, Berkeley (CA), 2000, pp. 59-82.

Flaherty, D., 'Privacy Impact Assessments: An Essential Tool For Data Protection', in *One World, One Privacy, Towards An Electronic Citizenship,* 22nd International Conference on Privacy and Personal Data Protection, Venice, 28-30 September 2000, pp. 77 - 86.

France, E., 'Using Design to Deliver Privacy', in *One World, One Privacy, Towards an Electronic Citizenship*, 22nd International Conference on Privacy and Personal Data Protection, Venice, 28-30 September 2000.

Gundermann, L., 'Das teledienstedatenschutzgesetzt - ein virtuelles Gesetz', in Bäumler, H. (ed.), *E-Privacy: Datenschutz im Internet*, Braunschweig: Vieweg, 2000, pp. 58-68.

Hes, R. and Borking, J., *Privacy Enhancing Technologies: The Path to Anonymity*, The Hague: Registratiekamer, 1998.

Kohntopp, M. and Pfitzman, A., *Datenschutz: Next Generation*, Kiel: Unabhängiges Landeszentrum für Datenschutz, Schleswig-Holstein, 1999.

Parliamentary Document 25 892 # 92c, Parliamentary Year 1999-2000, Memory of Reply to First Chamber regarding the WBP, p. 16. (Dutch Parliament).

Parliamentary Document 26 387, No. 15, Parliamentary Year 2000-2001 (Dutch Parliament).

Parliamentary Documents 25 892, no. 3, p. 98, Parliamentary Year 1997-1998 (Dutch Parliament).

Raab, C., 'Co-Producing Data Protection', *International Review of Law Computers & Technology*, 11, 1, 1997, pp. 11-24.

Raab, C.., 'Identity Checks - and Balances', in Bort, E. and Keat, R. (eds.), *The Boundaries of Understanding: Essays in Honour of Malcolm Anderson*, Edinburgh: International Social Sciences Institute, 1999, pp. 87-95.

Registratiekamer, *Advies Beveiliging Persoonsgegevens*, Rijswijk 1994.

Reidenberg, J., ‘Resolving Conflicting International Data Privacy Rules in Cyberspace’, in *One World, One Privacy, Towards An Electronic Citizenship*, 22nd International Conference on Privacy and Personal Data Protection, Venice, 28-30 September 2000.

Rosznagel, A., ‘Datenschutz-Audit’, *Datenschutz und Datensicherheit*, 9, 1997, pp. 505 - 515.

Rötzer, F., ‘Das recht auf Anonimität’, in Bäumler, H. (ed.), *E-Privacy: Datenschutz im Internet*, Braunschweig: Vieweg, 2000, pp. 27-34.

Schwartz, ‘P., Beyond Lessig’s *Code* for Internet Privacy: Cyberspace Filters, Privacy Control and Fair Information Practices’, *Wisconsin Law Review*, vol. 2000, No.4, pp. 743-88.

Syverson, P., Tsudik, G. *et al*., ‘Towards an Analysis of Onion Routing Security’, in *Proceedings of the Workshop on Design Issues in Anonymity and Unobservability*, Berkeley (CA), 2000, pp.83-100.

Tettero, O.*, Intrinsic Information Security: Embedding Security Issues in the Design Process of Telematics Systems*, Telematica Instituut Fundamental Research Series, No. 006, Enschede, 2000

Versmissen*,* J., *Keys of Trust: TTP Services and Privacy - The Judicial Preconditions Explored*, A&V Study No. 22, The Hague, 2001.

WBP Raamwerk Privacy Audit Alfa Version 4.0 (1/9/2000), Samenwerkingsverband Werkgroep Audit Aanpak, pp. 32-50.