

John J. Borking

Privacy Standards for Trust

The application of privacy enhancing technologies (PET) in different countries has proven that PET is a suitable tool for achieving advanced types of information exchange within legal privacy constraints and that it can be applied in all central databases, connected back-offices, clearing houses, information supply chains and local databases. However in order to achieve mass application and scalability of PET in information systems, the privacy principles as applied in the EU privacy protection directives and Fair Information Practices need to be standardized. This article points out the need for privacy standards, the consequences of the Wroclaw resolution adopted at the 26th International Conference of Data Protection and Privacy Commissioners, the necessity for a legal entity representing the privacy commissioners at the ISO level and the necessary steps to achieve a worldwide privacy standard in order to realize within a relatively short time for all world citizens a worldwide working built-in and preventive personal data protection.

Table of contents

1. Ten Years of Privacy Enhancing Technologies
2. The Need for Trust
3. The Importance of Privacy Standards for technology
4. The Wroclaw Resolution
5. The Impetus for the Establishment of Wroclaw Foundation
6. Countervailing Powers
7. Progress to date and vision
8. Conclusion

1. Ten Years of Privacy Enhancing Technologies

[Rz 1] On September 6, 1995 during the 17th International Conference on Data Protection in Copenhagen the concept of privacy enhancing technologies was introduced into the world of the privacy regulators¹. Privacy Enhancing Technologies (PET) is a common name for a range of different technologies to protect sensitive personal data within information systems. PET is more carefully defined as a coherent system of Information and Communications Technologies (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 information system². The National Consumer Council (NCC) in the UK agrees that there is considerable merit in the use of PET, particularly at the design stage of new systems and products. According to NCC governments in particular have a strong role to play in procurement exercises to ensure that they specify the use of PET in system design³. Utilization of PET signals trustworthiness and creates public confidence in the processing of their personal data in government and private sector information systems⁴.

2. The Need for Trust

[Rz 2] As information and communications technologies continue to advance, everything points in the direction of more, faster and more efficient service to the citizen and consumer. The 'one-to one' individualized approach in the marketing of goods and services and in the rendering of services by government and local authorities can only succeed if there is a high level of trust among government and the citizens and the suppliers and the consumers as well. Without trust virtually all of our social relationships would fail and it would become impossible to function normally. If we do not trust the shopkeeper to deliver the goods we paid for, then purchases would become very awkward. We make ourselves vulnerable to others every day, but we usually are comfortable in doing so because we trust that their actions will not be inappropriate or harmful. By trusting others to act as we expect them to act, we can reduce the things we have to worry about. Trust enables communication and cooperation between each other and often it is based on non-verbal body language in the real world. In the virtual world there are no such 'tangible'

signals. While surfing on the Internet the user exhibits behavior and conveys information that makes him or her vulnerable to someone else not under the control of the user. Privacy and data protection leads to trust, here to be defined as consumers' (citizens') thoughts, feelings, emotions, or behaviors that occur when they feel that an organization or individual can be relied upon to act in their best interest when they give up direct control.⁵

[Rz 3] The question of providing consumer trust in the ever increasing technology era we live in, is a complex one particularly when you include the effects ubiquitous Internet technologies have had on consumer preference and trust. It is a difficult and often impossible task for a consumer to be able to properly judge when trust should be granted when the company or government or individual collecting their personal information is not known, and will probably never be known. It is impossible for individuals to be able to effectively exercise control over their data after the trust has been granted. In a stable government environment, consumers rely on the ability of lawmakers and law enforcers to ensure that trust, once granted, is protected.

[Rz 4] Indeed, in the US, where needless to say, consumer rights are prevalent, in a hearing before the US Congressional Senate Committee Marc Rotenberg, of EPIC quoted the following:⁶:

- According to Forrester Research, 90% of Americans want the ability to control the collection and use of their data
- According to Business Week, three times as many Americans believe the government should pass laws now to safeguard online privacy as those who believe self-regulation is sufficient.
- According to the Pew Internet and American Life Project, more than 90% of Internet users thought companies should be punished when they violate their own privacy policies

[Rz 5] Consumers want to be protected, but are ill equipped to make sound and subjective decisions in the absence of standards.

3. The Importance of Privacy Standards for technology

[Rz 6] The application of PET in, Belgium⁷, Canada⁸, Germany⁹ and The Netherlands¹⁰ has proven that PET is a suitable tool for achieving advanced types of information exchange within legal privacy constraints and it can be applied in all central databases, connected back-offices, clearing houses, information supply chains and local databases¹¹. However in order to achieve mass application and scalability¹² of PET in information systems, the privacy principles PET protects that need to be standardized. Research undertaken by the Technical University Dresden aimed at identifying the economic effects of standardization for businesses and society as a whole¹³ shows not only that standardization leads to significant cost reduction, but also that standardization reduces the economic risk of R&D activities. The study proved that standards as a form of technology transfer have a positive influence not only on innovation (and that a lack of standards creates significant hurdles to innovation), and also that relevant standards for society lead to withdrawal of standards and practices that have outlived their technical, scientific or societal significance¹⁴. Privacy standards would promote built-in privacy protection and would wipe out products and services that lead to privacy intrusion. They would stimulate and open markets for new products and services with built-in privacy protection as well.

[Rz 7] In addition to this, there are more reasons why privacy standards are required and why it is very important to meet the challenge of developing a comprehensive set of privacy standards, namely:

- a) Reducing the cost of global compliance
- b) Reducing the risk of developing new technologies
- c) Increasing voluntary compliance
- d) Providing thought leadership in a scarce resource field
- e) Easing the cost of compliance

a) Costs of global compliance

[Rz 8] Due to the fact that we live in a global community, vendors, users and governments cannot operate in isolation. The Privacy domain is increasingly becoming a legislated area many different countries in the world. Multiple national legislations result in costs of compliance. The EU has solved this issue with its privacy directives and because of the work of the WP article 29 the legislation of the member states is harmonized throughout the EU. Outside of the EU, there is a proliferation of legislation, some of which is substantially similar with the EU directives and some of which is not. However, in the creation of global standards, the legislation can and should be broken into key components that in turn can be used as the basis for writing a framework for privacy standards. Harmonization of the fair information practices is the vehicle to achieve this.

b) Reducing risk of developing new technologies

[Rz 9] Privacy standards are required to ensure that costs are managed in developing new technologies and that a level playing field is developed to ensure innovative solutions can be developed by small, medium and large companies. Standards are critically important in ensuring that all innovative developers of new technology are given the tools they need to build their products and services solutions. With detailed standards, comes the ability to build to those standards and the innovation will lie with the implementation and the solutions that address the same set of standards.

[Rz 10] Developing technology in an area that does not have standards is extremely risky. In the absence of standards, vendors and innovators are left to guess at legislative interpretations. If they guess incorrectly, their technologies may not be compliant and their resources have been wasted. If standards are available, they are left to address those standards rather than guessing about whether their solutions will be compliant or not.

[Rz 11] Standards also reduce the time to market. Innovators can rely on comprehensive global standards and not waste time or resources on developing their own standards and obtaining buy in for the newly developed standard.

[Rz 12] Developing detailed standards levels the field for all size of companies. Medium and small companies typically do not have the resources to develop standards, and yet they have innovative ideas that they wish to develop and market. Alleviating this cost for small and medium size companies allows them to use scarce resources to further their innovations.

[Rz 13] Lastly, in the absence of detailed standards, there is a danger of large company solutions dominating the marketplace, as they essentially build solutions in an attempt to become the standard. Proprietary standards owned by one or a small group of companies are not in the best interests of a competitive marketplace.

c) Voluntary compliance

[Rz 14] Voluntary compliance is essential to the implementation of legislation. Voluntary compliance is very difficult for vendors in the field of technology, given the complexity of understanding multiple applications of multiple legislations.

[Rz 15] Legislators can assist in promoting and ensuring voluntary compliance by developing detailed and comprehensive standards and guidelines. Furthering the compliance can be eased through cost reduction in implementation.

d) Providing thought leadership

[Rz 16] Providing thought leadership in the field of privacy technologies is an essential ingredient for the implementation of mass application and acceptance of Privacy Enhancing Technologies (PET). PET is an emerging field and not unlike other areas of emerging technologies, there is a scarcity of resources in this area. There is a critical mass of knowledge and resources within the Privacy and Data Protection Authorities and both the groups and individuals that have emerged out of previous commissions' staff, and partner companies. This critical mass is required to further the proper and appropriate writing of technologies standards for PET.

[Rz 17] In the absence of this highly skilled resource base, the development of these standards may end in the

promotion of standards that do not meet the requirements as outlined in the law such as was the case of the ISTPA framework. Of course, if privacy standards are developed through this critical mass of resources, the assistance and cooperation of these groups can be readily realized and transfer of skills to these groups will result in successful implementation of a comprehensive set of standards.

e) The cost of compliance

[Rz 18] The cost of compliance can be onerous, if compliance mechanisms are not thoroughly outlined and detailed. There are few, if any laws that detail how technology solutions can be implemented to meet legislated requirements. PET standards will provide the standards for compliance and reduce the cost of compliance by outlining how technologies can be developed to ensure legislated requirements are met.

[Rz 19] During the years that the Registratiekamer (Dutch data protection authority, since 2001 named: College bescherming persoonsgegevens) advised and strongly promoted the use of PET in information systems of the government, vendors of ICT systems saw market opportunities of their own products claiming PET features, that after time consuming investigation of the Registratiekamer weren't available or only applied partly and in a wrong way. IT then became clear for the Registratiekamer that there was a lack of general accepted PET evaluation tools for testing and assessing the privacy functionality of systems. This lack of evaluation tools led in 2000 to the establishment of a working research party named PETTEP (Privacy Enhancing Technologies Testing and Evaluation Project), a joint project of Information and Privacy Commissioner in Toronto, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein in Kiel and the registratiekamer in The Hague. In March 2001 IPC started developing a set of privacy protection profiles as enlargement of the Common Criteria for Information Technology Security Evaluation on anonymity, pseudonymity, unlinkability and unobservability¹⁵. The strict and literal interpretation of certain provisions of the directive 95/46/EC and applicable national data protection law has the potential to actually threaten the advancement of anonymization and pseudonymization as practical ways to protect personal data. Over the years the need for a standardized tool and test for anonymization of personal data became urgent as well¹⁶.

[Rz 20] The last and perhaps most significant aspect of the need for developing privacy standards, is the theory advanced by Lawrence Lessig that «Code is Law». Lessig is a leading thinker from Stanford University, in the area of constitutional law and has made several arguments for the basis of viewing computer code as the law. Lessig pointed out that in the real world we recognize how laws regulate through constitutions, statutes and other legal codes. In cyberspace we have to understand how the software and hardware that make cyberspace regulate this space. Therefore his famous adage is: Code is Law!¹⁷ But we don't know what values are protected by this Code. Is privacy as a human right preserved for every user of the Internet? We know that because of the tracking of the user's clicks and web data mining this isn't fact at all. In order to have built-in privacy protection online and offline preventing privacy intrusions, it is necessary to build into the Code standardized privacy protection rules. Code is written by developers and shaped by standards, but privacy standards don't exist. There isn't a privacy standard that can serve as a model for developers of hardware, firmware and software. As cyberspace doesn't take care of itself, we have to influence code writers. Four constraints regulate the architecture of cyberspace: Software and Hardware (the Code), Law, Norms and Market. Changes in any one will affect the regulation of the whole¹⁸. ISO standards work as norms worldwide and are closest to the reality of the developers of the architecture. Ergo: if we sincerely want a well balanced¹⁹ globally enforced privacy protection then a model privacy standard based on translated EU privacy directive 95/46/EC and 2002/58/EC and the FIPs²⁰ have to be developed and adopted by the code writers, This is a much better approach than trying to create a multinational law that regulates worldwide the Code with regard to privacy protection. This isn't only time consuming (we haven't enough time) but due to the enormous cultural differences in our world totally unfeasible. If Lessig theories are in fact of any relevance at all, the importance of privacy standards takes on a dramatic and essential meaning in ensuring compliance of the application and development of Code.

4. The Wroclaw Resolution

[Rz 21] In 2004 the privacy protection community was confronted with a Draft Privacy Framework Standard developed by the industry group: International Security, Trust & Privacy Alliance (ISTPA)²¹. ISTPA and its partners

aim to make the Framework a comprehensive and valuable aid for those implementing privacy policies in information systems containing personally identifiable information. The submission of the ISTPA Privacy Framework by the International System Security Engineering Association (ISSEA) as a candidate for an ISO Publicly Available Specification («PAS») triggered international discussion about the need for such standards to support the compliance efforts of privacy officers and «business owners» in both the public and private sectors, as well as those implementing relevant information systems or designing products for their use. The initial problem identified by several European and Canadian Privacy Commissioners was that ISTPA did not satisfy FIPs & EU Privacy legislation. More research demonstrated that problem went far deeper than one single standard that did not meet legislation. More serious issues were that standards with privacy relevant components were not being vetted by the legal authorities mandated with implementation and enforcement of privacy legislation, and therefore had inaccuracies, and moreover privacy standards were developed within security frameworks.

[Rz 22] As a direct response to this PAS during the 26th International Conference on Privacy and Personal Data Protection in Wroclaw, the International Conference of Data Protection and Privacy Commissioners supporting the development of an effective and unanimously accepted international privacy technology standard adopted the following resolution²²:

[Rz 23] The Resolution outlined the following:

- The development of privacy enhancing technology standards supporting the implementation of legal rules on privacy and formulating of such rules where they are lacking²³;
- For future international standards: Legislation to be taken into consideration, specifically the Fair Information Practices and the concepts of data scarcity, minimization and anonymity²⁴;
- The establishment of a new Sub Committee for the development of IT standards regarding privacy²⁵;
- A request for JTC1 SC27 to withdraw the ISTPA framework as publicly available specification (PAS) standard and suspend any existing PAS submissions for fast-track procedure and adoption in the field of privacy and data protection²⁶;
- Inclusion of the Privacy Enhancing technology Testing & Evaluation Project (PETTEP)²⁷ as official liaison organization to the ISO JTC1 Privacy Technology Study Group (PTSG)²⁸;
- Encouraging the Data protection Commissioners to join PETTEP, allowing them as PETTEP members to have an immediate voice in the discussions regarding the development of an ISO privacy technology standard²⁹.

[Rz 24] However the execution of the resolution proved not to be simple, for the letters sent from the Chair of the Conference Dr Ewa Kulesza to the Chair of JTC1 attaching the resolution and suggesting next steps, weren't circulated to National JTC1 Bodies for consideration, nor was its contents made known, due to JTC1 rules of operation. The result was that not only were the goals of the resolution unknown, but also they were not met. However after much lobbying and just a week before the final vote in ISO ISTPA withdrew the draft privacy framework and the fast-track procedure was stopped on a voluntary basis. It should be noted that this was achieved outside of ISO, since the rules of JTC1 did not allow for any input from the Conference, and the recommendations of the PTSG where PETTEP did have input, were not passed at the plenary session of the JTC1 in Berlin in October 2004. It should be noted as well that no check and balances have been noted or discussed or implemented in regards to paragraph 10 of the resolution, where future standards are being submitted and are progressing through JTC/ISO without the mentioned controls being implemented.

[Rz 25] ISTPA proposed in May 2005 to its members the revision of the ISTPA Privacy Framework as ISSEA's submission of the ISTPA Privacy Framework as a candidate ISO Publicly Available Specification («PAS») triggering more international discussion, especially with regard to the «collection limitation» principle of fair information practices. The revision would make it clearer how the Framework supports the implementation of internationally accepted principles of fair information practices and precisely where the Framework fits into an organization's efforts to plan, implement, and verify compliance with all applicable privacy requirements arising from law, contract, or internal policies. This is seen to be a very positive move towards cooperative development of compliant privacy standards, with the Wroclaw Foundation providing the leadership and knowledge in developing appropriate standards.

5. The Impetus for the Establishment of the Wroclaw Foundation

[Rz 26] As per the request in paragraph 7 of the resolution, PETTEP was requested to adopt the Conference's resolution and to present them to the PTSG at the earliest possible date. The members of PETTEP accepted the responsibilities of its proposed role under the resolution.

[Rz 27] It became very clear during the lobbying for withdrawal of the ISTPA PAS that PETTEP could not meet the demands as outlined in the resolution. A privacy standard was proceeding even though the legal authorities had outlined inherent problems with the standard, the legal authority of the Commissioners regarding enforcement of legislation was not recognized by ISO and the Privacy Commissioners were unable to stop or even to alter the acceptance of the PAS and had no meaningful role in the standards process and privacy standards were being addressed by security subcommittees of the national standards organizations within security frameworks.

[Rz 28] A more formal structure for PETTEP was necessary to address the ISO requirement for liaison status, and although the PTSG had recognized the importance of including the input from privacy legal authorities, as noted in the resolution, ISO/JTC1 has a more formal and structured set of rules and could not and did not allow for any input from the Conference.

[Rz 29] It was discussed and highlighted by the Secretary of JTC1, Mr. Michael Smith, that each individual Commission could join their ISO national body and try and exert influence through their existing subcommittees of JTC1. Once they became members it is up to the discretion of each national body to allow for the input and to weigh the input with other objectives of their national body and further within their subcommittees, and finally within JTC1 itself. This approach was identified as being impractical and ineffective given the resources afforded to the Commissioners. Furthermore, it was very difficult to envision how the goals of the resolution in developing global standards would be met through this approach. The alternative proposed was to form a formal structured group to represent the Conference, as a structured group that would in fact qualify under the rules of JTC1 and whose input as a legal entity would be recognized.

[Rz 30] To meet the demanding requirements of JTC1/ISO the Wroclaw Foundation was formed on January 7, 2005 as the successor of PETTEP to address the underlying issues and reasons for the dismissal by ISO of the resolution. The Wroclaw Foundation was named after the city where the resolution that had been passed and to extend tribute to the work of Dr Ewa Kulesza and her organization in furthering the resolution. The foundation is a legal entity under Dutch law³⁰ and protects the board members against liabilities, provided the articles of association are adhered to. Its articles of association also warrant the democratic adoption of the proposed privacy standards within the management board before submitting it to ISO as a PAS. The Foundation in forming the legal structure also gave the members of PETTEP and their member Commissions a more formal and structured way of effectively addressing the goals of the resolution, which met the identified issue of scarcity of resources.

[Rz 31] The Interim board decided that the acronym PETTEP will be registered as trademark and that the individual members of PETTEP will continue their work as designated to the group under the auspices of the Wroclaw Foundation. The membership for the Foundation was opened to all Commissioners, and remains open to all members of the Conference. The fulfillment of the resolution is being met through leadership of the following board members: the Privacy Commissioners of Poland, Czech Republic, Bundesbeauftragter für den Datenschutz of Germany, the Beauftragter für Datenschutz und Informationsfreiheit of Berlin and the Landesbeauftragte für den Datenschutz Schleswig-Holstein, Privacy Commissioner of Spain, Federal Privacy Commissioner of Canada and the Information and Privacy Commissioner of Ontario, Belgium, Estonia and Luxemburg.

[Rz 32] In acknowledging the scarcity of resources and in acknowledging the differing mandates of the Commissioners, the Foundation has proposed a structure to meet these requirements. The main body of the Wroclaw Foundation is the Management Board³¹. The Board is mandated to carry out the resolution. There are two Committees of the Foundation³² that can be used to seek resources from the privacy community to further the work of the Foundation and these are the Committee of Experts for content, and the Liaison Committee for lobbying. Their mandates are not yet formalized.

[Rz 33] Finally, the reality of the costs of carrying out the resolution demands is being examined within the context

of the economic constraints of the Commissioners. The Foundation's articles of association do contemplate an enterprise at arm's length³³, and will further examine whether such an enterprise is necessary for the fulfillment of the resolution.

[Rz 34] The mandate for Wroclaw Foundation was taken from the resolution and can be summarized as follows:

1. To develop model privacy technology standard within both content and organizational frameworks that are distinct, and unique to privacy and that enforce privacy legislation as outlined in the Fair Information Practices and EU privacy legislation as «checklist» for every standard
2. To enable Privacy and Data Protection Commissioners to have a meaningful and substantial role in the writing and approval of privacy standards to prevent privacy invasive standards
3. To develop meaningful representation of the Commissioners at ISO level and partnership with ISO and other standards bodies to further the standards work.

[Rz 35] Two ISO organizations, JTC1 and COPOLCO have invited the Foundation to participate as a liaison body. Most certainly positive progress is being made. The Foundation is providing the leadership necessary for cooperative development of privacy standards, within legislated frameworks.

6. Countervailing Powers

[Rz 36] There are certainly vendors that resist the development of standards. Competitive forces in market for technology vendors, may work against the development of generic standards. Larger vendors may see advantages in the development of proprietary standards that can then be used to capture market share. Vendors guard their research, including standards development closely, in order to provide window of opportunity for gaining market share through advanced product development. Cost factors may drive budgets expenditures away from standards development and may result in vendors relying on either government or standards organizations such as ISO for the development of standards, or may result in substandard products being developed that do not comply with eventual privacy standards.

[Rz 37] One additional factor needs examination, and that is the current volatility of the privacy standards arena has resulted in some major vendors taking a «lets wait and see» attitude. Large organizations, in particular, may wait to make decisions on joining standards organization, until the organizational structures of the privacy standards organizations are completed, and coordinated by a central authority, which is indeed acknowledged as an authority. The proliferation of the privacy private sector standards organizations is working against the writing of generic global standards, as each organization tries to gain the upper hand in writing privacy standards that can be used for market advantage. Certainly the formation of a privacy standards organization such as Wroclaw Foundation and the firm support of the Commissioners behind the foundation will solve this problem.

7. Progress to date and vision

[Rz 38] A joint PETTEP/ISO effort to compile existing legislations was undertaken through the PTSG, and the end result showed significant amounts of legislation have been enacted throughout the globe. This list was submitted to the PTSG and has further been published through JTC1, and also through PETTEP members. There has been no work completed on the list since its inception, but JTC1 should be encouraged to complete the list and update it. PETTEP has produced substantive work on the extension of the Common Criteria but still very much has to be done. This has led to a number of conflicts being identified in the security standard, and has demonstrated that the Common Criteria is not the place to start developing privacy standards. I believe that a faster way to achieve a privacy standard is to first produce a globally harmonized set of Fair Information Practices. The next steps are as follows:

[Rz 39] Line of Development from Privacy Law into Privacy Standards:

- 2006/7
 - Harmonized set of Fair Information Practices
 - Working draft of a Global Privacy Standard Framework (Pre-PAS submission)
 - Develop working relationships with ISO, other partners
- 2007/8
 - A streamlined cost effective PET evaluation methodology to be used by public and private sector for designing & deploying personal data processing systems
- 2008/11
 - ISO Comprehensive set of privacy standards
 - Comprehensive, global accreditation authority, model and process based on the set of privacy standards

8. Conclusion

[Rz 40] Technology developers essentially have the power to implement privacy protective technology or not. The implementation of privacy legislation in technology is achievable, however the lack of privacy standards and detailed guidelines are preventing this. Privacy standards are pivotal to a worldwide privacy protection online and offline.

[Rz 41] The many initiatives that have been and are being undertaken, as exemplified by the ISTPA framework project, demonstrate that in the absence of standards, indeed vendors are proceeding to develop their own version of standards. In the absence of the involvement of a cohesive body representing the legal authorities, there is a danger that these standards developed will again not meet legislation. The Privacy Commissioners have it well within their ability to provide the leadership required to develop a complete set of privacy legislation compliant standards.

[Rz 42] Two ISO organizations, JTC1 and COPOLCO have invited the Foundation to participate as a liaison body. Most certainly positive progress is being made. The Foundation is providing the leadership necessary for cooperative development of privacy standards, within legislated frameworks.

[Rz 43] It is a sine qua non that a model privacy standard and a PET evaluation standard has to be developed and standardized if we want within a relatively short time for all world citizens a worldwide working built-in and preventive personal data protection.

Drs John J. Borking (Dutch Nationality) is Director of Borking Consultancy (Wassenaar). He is participating in several EU funded research projects doing research on «translating» privacy law into code, privacy ontologies, privacy standardisation and privacy management systems

- ¹ Borking, John J., Back to Anonymity – Privacy Enhancing Technologies, Based on a joint study in The Netherlands and Ontario (Canada), in Proceedings of the 17th International Conference on Data Protection, Registertilsynet, Copenhagen 1995 p.214- 242
- ² Borking, J.J., Raab, C., Laws, PETS and other technologies for privacy protection, *Journal of Information, Law and Technology*, no. 1, February 2001.
- ³ Lace, Suzanne, The Glass Consumer, life in a surveillance society, Bristol 2005 p.218
- ⁴ Koorn, R., Borking J.J. et al. Privacy-Enhancing Technologies, White Paper for decision-Makers, Ministry of Interior and Kingdom Relations, The Hague 2004. p. 5
- ⁵ A. Patrick, Privacy, Trust, Agents & Users: A Review of Human-Factors Issues Associated with Building Trustworthy Software Agents Ottawa 2001, – EU-PISA project Delivery Document D 22 at www.pet-pisa.nl .6 Paper685, www.sans.org/rr/whitepapers/privacy/685.php
- ⁶

- A. Patrick, Privacy, Trust, Agents & Users: A Review of Human-Factors Issues Associated with Building Trustworthy Software agents Ottawa 2001, – EUPISA project Delivery Document D 22 at www.pet-pisa.nl
- 7 De Meyer F, B. Claerhout, G.J.E. de Moor., The PRIDEH project: taking up Privacy Protection Services in e-Health. Proceedings MIC 2002 «Health Continuum and Data Exchange». IOS Press, 2002, blz. 171-177.
- 8 Zero-Knowledge-Systems Inc.: www.freedom.net/
- 9 Hansen M., P. Berlich, J. Camenisch, S. Clauß, A. Pfitzmann, M. Waidner: Privacy-Enhancing Identity Management; Information Security Technical Report (ISTR) Volume 9, Issue 1 (2004), Elsevier, UK, p. 35 – 44, [http://dx.doi.org/10.1016/S1363-4127\(04\)00014-7](http://dx.doi.org/10.1016/S1363-4127(04)00014-7).
- 10 Koorn, R.F., H. van Gils, J. ter Hart, P. Overbeek, R. Tellegen, J.J. Borking, Privacy-Enhancing Technologies, White Paper for Decision-Makers, Dutch Ministry of Interior and Kingdom Relations, The Hague 2005, p.. 21 – 33.
- 11 Koorn, R., Borking J.J. et al. Privacy-Enhancing Technologies, Witboek voor beslissers, op.cit. p 27-46
- 12 A PET solution is scalable, means that when the size of the problem is increased e.g. more users take part, the PET solution does not require a disproportional amount of resources e.g. network resources needed for communications between software agents
- 13 Bahke, T. e.a. The Economic Benefits of Standardization, Dresden/Karlsruhe, April 2000
- 14 See Summary of The Economic Benefits of Standardization, Dresden/Karlsruhe, April 2000, p.20-22 and 27-29
- 15 Van Blarkom G.W., Borking, J.J., Olk, J.G.e., handbook of Privacy and Privacy-Enhancing Technologies, the casr of Intelligent Software Agents, ISBN 90-74087-33-7 The Hague 2003 p.42-50; See also ISO 15408
- 16 See Document CEN WS DPPN-0061 (2005), John Borking & David Trower, Legal Study On The Effective Anonymisation & Pseudonymisation Of Personal Data and The Demarcation Line (Threshold) Between Identifiable And Non-Identifiable Data
- 17 Lessig, L., Code and other laws of cyberspace, New York 1999, p.6
- 18 Lessig, op.cit. p. 87- 88
- 19 Lessig,op.cit. p. 142: «The code has already upset a traditional balance»
- 20 For example the Canadian Free Information Practices
- 21 www.istpa.org
- 22 <http://26konferencja.giodo.gov.pl/rezolucje/j/en>.
- 23 Resolution reference paragraph 1
- 24 Resolution reference paragraph 2
- 25 Resolution reference paragraph 4
- 26 Resolution reference paragraph 8.9.10
- 27 PETTEP is a project led by the Ontario Information & Privacy Commissioner together with Unabhängiges Landeszentrum Für Datenschutz Schleswig-Holstein that has undertaken research and analysis in developing testing and evaluation criteria for privacy information technology and information systems.
- 28 Resolution reference paragraph 5
- 29 Resolution reference paragraph 6
- 30 The foundation is registered in the Chamber of Commerce’s Register for Foundations under file number Kamer van Koophandel Haaglanden # 27273640
- 31 Article 3 of the Articles of Association
- 32 Article 10 of the Articles of Association
- 33 Article 2 g of the Articles of Association

Rechtsgebiet: Datenschutz
Erschienen in: Jusletter 3. Oktober 2005
Zitervorschlag: John J. Borking, Privacy Standards for Trust, in: Jusletter 3. Oktober 2005
Internetadresse: <http://www.weblaw.ch/jusletter/Artikel.asp?ArticleNr=4237>