Privacy Enhancing Technologies

State of the Art Review

Version 1: February 2002

Contents

Background

Privacy and anonymity are increasingly important in the online world. Corporations and governments are beginning to realise their power to track users and users are increasingly demanding protection of privacy.

According to Fischer-Hubner privacy protection can be achieved by: (i) privacy and data protection laws promoted by government, (ii) self-regulation for fair information practices by codes of conduct promoted by businesses, (iii) privacy enhancing technologies adopted by individuals and (iv) privacy education of consumers and IT professionals.

Consumer polls have repeatedly shown that individuals value their privacy and are concerned about the fact that so much personal information is routinely stored in computer databases over which they have no control. Protecting one's identity goes hand in hand with the option to remain anonymous, a key component of privacy. While advances in information and communications technology have fuelled the ability of organisations to store massive amounts of personal data, this has increasingly jeopardised the privacy of those whose information is being collected. Minimising the amount of identifying data could restore privacy considerably, but would still permit the collection of essential information.

What is needed is a paradigm shift away from a more-is-better mindset, to a minimalist one. The technology needed to achieve this goal exists today, known as Privacy Enhancing Technologies, permitting one to engage in transactions without revealing one's identity, for example, by introducing the concept of an identity protector. The notion of pseudonymity has also been introduced as an integral part of protecting one's identity. These technologies are available; what is needed is the will to implement Privacy Enhancing Technologies instead of applying tracking technologies, as is common nowadays [Hes].

The Past: Technologies related to privacy protection

The term “privacy enhancement” has been used for more than a decade to represent an array of related technologies concerned with various aspects of Internet security.

According to Roger Clarke [Clarke] the term “Privacy Enhanced Mail” (PEM) was used at least as early as the mid-1980s, in the RFC series 989 (February 1987), 1040 (January 1988), and 1113-1115 (August 1989), which defined a “Privacy Enhancement for Internet Electronic Mail” [Linn]. The term referred, however, only to the narrow concept of message transmission security, and its requirements of confidentiality, authentication, and message integrity assurance. The much broader concept of “Privacy Enhancing Technologies” (PETs) has been around since at least the mid-1990s. Ann Cavoukian in Toronto and Peter Hustinx in Amsterdam used it as the title of a joint work in 1995 along with EPIC's Marc Rotenberg in Washington DC. Roger Clarke originated the neologism “Privacy Invasive Technologies” (PITs) in late 1998. The notion of “Privacy Sympathetic Technology” (PST), was used as a means of distinguishing between tools for anonymity (PETs) and those for pseudonymity (PITs) [Clarke].

The above technologies could be classified as (i) Ads blocking/Cookie crushing, (ii) Anonymous browsing and (iii) Secure email [Garfinkel]. Some examples include AdSubtract, Internet Junkbuster Proxy, Freedom Internet Privacy Suite, Norton Internet Security, WebWasher, Anonymizer, Freedom, safeWeb, HushMail and Omniva.

PETs defined. Why we need them? How we use them?

Security and privacy enhancing technologies are already available. However, whilst the use of security measures to prevent unauthorised access to personal data is an important component of privacy, it does not equal privacy protection. The Office of the Information Commissioner (OIC) argues that the latter starts by ensuring that data collection is necessary and that using the collected information is legitimate. They recognise that “a comprehensive approach would be to seek out ways in which technology may be used to enhance the protection of information privacy or data protection”. PETs are innovative software-based mechanisms that have the potential to encode or facilitate each of the above aspects of Data Protection Law [Jackson]. Additionally, the term PETs may be used to refer to a variety of technologies that safeguard personal privacy by minimising or eliminating the collection of identifiable data [Hes].

According to Sottong-Micas and Hillbrand PETs could be considered as providing a competitive advantage because they increase users’ trust in the services and technologies involved [Sottong-Micas]. On 20th October 1999 the Internal Market DG contributed to the organisation of a workshop on the Data Protection Directive and Technology held under the auspices of DG Information Society’s Telematics Programme. The Internal Market DG proposed to integrate into standardisation initiatives the idea of schemes of verification and certification for existing products and those under development for compliance with the Data Protection Directive. It defended the idea of a “one-stop-shop” for this concept of PETs within the Information Society Technologies Programme with a view on improving transparency and access for interested parties [http://www.cordis.lu/ist] [http://www.concord.cscdc.be/meetings.php3].

These facts underline a need for PETs so as to protect (i) the user identities providing anonymity, pseudonymity, unlinkability, unobservability of users, (ii) the user identities providing anonymity, pseudonymity of data subjects and (iii) the confidentiality and integrity of personal data [Fischer-Hubner].

Agre regards PETs as one of the most significant technical innovations, since beginning with the publication of the first public-key cryptographic methods in the 1970s. Mathematicians have constructed “a formidable array of protocols for communicating and conducting transactions while controlling access to sensitive information” [Agre]. The application of advanced mathematics to the protection of privacy disrupted the conventional pessimistic association between technology and social control. This view is strongly supported by Burkert’s observations that “no longer are privacy advocates in the position of resisting technology as such, and no longer can objectives of social control be hidden beneath the mask of technical necessity" [Burkert].

There is significant literature regarding privacy risks and threats such as profiling, data marketing, privacy invasion, cookies and tracking [Goldberg, Jackson, Nilsson]. These threats in a way dictate the main patterns of usage for PETs, which according to the Joint Research Centre are categorised as products for providing consumer choice (e.g. P3P, OPS) and protection mechanisms (e.g. Anonymity, Firewalls, Encryption, Cookie Crushers).

Protecting user identities with PETs

PETs can be used for protecting user identities by providing [Fischer-Hubner]:

(i) Anonymity (i.e. ensure that a user may use a resource or service, send or receive a message without disclosing her identity).

(ii) Pseudonymity (i.e. ensure that a user acting under a pseudonym may use a resource or service without disclosing her identity).

(iii) Unlinkability (i.e. ensure that the user may make use of resources or services without others being able to link these uses together, also senders and recipients cannot be identified as communicating with each other).

(iv) Unobservability (i.e. ensure that a user may use a resource or service without others being able to observe that the resource or service is being used).

According to Fischer-Hubner PETs can provide protection for User Identities at communication level, system level, application level and in audit trails. Some PETs lying under this category are: DC nets, MIX nets, Anonymous Remailers and Browsers, Onion Routing, Freedom Network, ISDN-Mixes, Digital and Blind Signatures, Ecash, Anonymous Payment Protocols, Pseudonymous Auditing and Trusted Third Parties.

A **digital signature** is the electronic equivalent of a handwritten signature. Just as a signature or personal "seal" on a document is proof of its authenticity, a digital signature provides the same, if not better, authentication. It provides the necessary assurance that only the individual who created the signature could have done so, and it permits all others to verify its authenticity. A particular type of encryption, public key encryption, considered to be an extremely reliable and secure form of encryption, forms the basis for digital signatures [Hes].

The **blind signature**, created by David Chaum of Digicash, is an extension of the digital signature, but with one critical feature added: it ensures the anonymity of the sender. While digital signatures are intended to be identifiable and to serve as proof that a particular individual signed a particular document, blind signatures provide the same authentication, but do so in a non-identifiable manner. The recipient will be assured of the fact that the transmission is authentic and reliable, but will not know who sent it. One application involving blind signatures is the use of digital cash, which may be used as an electronic form of payment that can be transmitted over computer networks. Just as cash is anonymous, digital cash is anonymous in that it cannot be traced back to a particular individual, it is considered to be unconditionally untraceable. However, the service provider is assured of its authenticity; all that is missing is the ability to link the transaction with a particular person [Chaum-a, Hes].

A **digital pseudonym** is a method of identifying an individual through an alternate digital or pseudo-identity, created for a particular purpose. It permits users to preserve their anonymity by concealing their true identities. While users, are not known to service providers in the conventional sense, they are, nonetheless, known by their pseudonyms for the purposes of conducting transactions. Digital pseudonyms are built upon the blind signature technique. However, in this instance, it is the service provider who assigns privileges to a given pseudonym (user) by creating a blind signature [Hes].

A **trusted third party** is an independent third party who is trusted by both the user and service provider alike (comparable to a digital attorney). This party can be entrusted with keeping such things as the master key linking digital pseudonyms with the true identities of their users. The trusted party knows that the relationship between a user's true identity and his/her pseudo-identity must be kept completely secret. However, if certain conditions require it, the trusted party will be permitted to reveal the user's identity (under previously agreed upon terms) to a service provider. The conditions under which an individual’s identity would be revealed must be known to both user and service provider prior to entering into an agreement with the trusted party [Hes].

The newest and most sophisticated **remailer** technology is the **Mixmaster**. They provide enhanced protection against eavesdropping attacks. Firstly, one always uses chaining with each link of the chain being encrypted. Secondly, such remailers use constant-length messages, to prevent passive correlation attacks where the eavesdropper matches up incoming and outgoing messages by size. Third, these remailers include defenses against sophisticated replay attacks. Finally, they offer improved message reordering code to stop passive correlation attacks based on timing coincidences. Because their security against eavesdropping relies on ``safety in numbers" (where the target message cannot be distinguished from any of the other messages in the remailer net), the architecture also calls for continuously-generated random cover traffic to hide the real messages among the random noise [Chaum-b, Cotrell, Goldberg].

Another technology is that of the “newnym”-style **nymservers**. These nymservers are essentially a melding of the recipient anonymity features of a anon.penet.fi style remailer with the chaining, encryption, and other security features of a cypherpunk-style remailer: a user obtains a pseudonym (e.g. joeblow@nym.alias.net) from a nymserver; mail to that pseudonym will be delivered to him. However, unlike anon.penet.fi, where the nymserver operator maintained a list matching pseudonyms to real email addresses, newnym-style nymservers only match pseudonyms to “reply blocks”": the nymserver operator does not have the real email address of the user, but rather the address of some remailer, and an encrypted block of data which it sends to that remailer. When decrypted, that block contains the address of a second remailer, and more encrypted data, etc. Eventually, when some remailer decrypts the block it receives, it will get the real email address of the user. The effect is that all of the remailers mentioned in the reply block would have to collude or be compromised in order to determine the email address associated with a newnym-style pseudonym [Goldberg].

Anonymous **digital cash** is another state-of-the-art technology for Internet privacy. As many observers have stressed, electronic commerce will be a driving force for the future of the Internet. Therefore, the emergence of digital commerce solutions with privacy and anonymity protection is very valuable. DigiCash's **ecash** [Chaum-c] has the strongest privacy protection of any deployed payment system--it uses sophisticated cryptographic protocols to guarantee that the payer's privacy is not compromised by the payment protocol even against a colluding bank and payee. Thus, DigiCash's ecash has many of the privacy properties of real cash; most other deployed payment systems have only about as much privacy as checks or credit cards [Goldberg].

Adams and Sasse believe that most invasions of privacy are not intentional but due to designers' inability, to anticipate how this data could be used, by whom, and how this might affect users. This problem is addressed by a model of user perceptions of **privacy in multimedia environments** [Adams-a]. This model has identified three major privacy factors namely information, sensitivity, receiver and usage that interact to form the users' overall perception of privacy.

A different more technical approach to dealing with trust as a security instrument was elaborated by Blaze et al, who subdivided trust management into different categories, such as authorisation, or the positive identification of **trusted parties**. They also introduced a trust management system to formulate trust and security policies for various applications, such as email, content-labelling and electronic licensing [Blaze]. A more specialised system, which uses digital signatures in web applications, is the REFEREE trust management system. A profile language is used to formulate trust policies [Chu, Kohntopp].

Anonymous Proxies (Trusted Third Parties) is another available technology for privacy enhancement. The principle of Trusted Third Parties (TTP) is simple - both users and commercial organisations create an account with a "trusted" Internet Service Provider. At this site, a user can register his personal details with assurance that they will not be passed onto other parties or used for marketing purposes. From this site a number of pseudonyms or 'aliases' can be created, which the user can use whilst carrying out transactions on the web. In some cases models have been proposed where it is possible to have purchasing powers arranged via the trusted third party, such that web based transactions can be charged indirectly to the client via the

TTP accounts. The weakness of TTP systems is establishing the credibility and trust of the third party provider [JRC].

Finally, **Anonymous/Pseudonymous servers** have been established on the Internet allowing users to set up anonymous e-mail accounts. Each anonymous account is assigned a unique ID so that recipients can respond to an anonymous email message. The servers provide accounts for both email and Usenet (newsgroups) activities and web browsing activities [JRC].

Personal Data Protection through PETs

According to Fischer-Hubner there are three types of PETs for protecting personal data: (i) Security Models enforcing legal privacy requirements, (ii) Cryptography and (ii) Steganography. There are several basic privacy requirements such as necessity of data collection and processing, purpose specification and binding and adequate organisational and technical safeguards. Steganography can be defined as the method of transmitting secret messages through innocuous carriers in such a way that the very existence of the embedded message is undetectable. There are two variants of steganographic systems with different intends. Digital steganography is used to conceal a message in a cover, where that hidden message is the object of communication. Digital watermarking is used to embed copyright, ownership and license information in a cover, where that cover is the object of communication [Fischer-Hubner]. These effects are even more intense in global wireless communication, where traffic data and possibly further personal user characteristics that are transferred with messages, and also user data inside content, can be collected at different sites and used to create communication or user behaviour profiles [Nilsson].

The **Platform for Privacy Preferences Project** (P3P), developed by the World Wide Web Consortium, is emerging as an industry standard providing a simple, automated way for users to gain more control over the use of personal information on Web sites they visit. At its most basic level, P3P is a standardised set of multiple-choice questions, covering all the major aspects of a Web site's privacy policies. Taken together, they represent a clear snapshot of how a site handles personal information about its users. P3P-enabled Web sites make this information available in a standard, machine-readable format. P3P-enabled browsers can "read" this snapshot automatically and compare it to the consumer's own set of privacy preferences. P3P enhances user control by putting privacy policies where users can find them, in a form users can understand, and, most importantly, enables users to act on what they see [Nilsson]. P3P focuses on privacy practice disclosure with respect to data collected through web interactions with merchants. It is designed to help users reach a semi-automated agreement with online merchants with regard to the processing of an individual's personal data. It does not exclude the use of other privacy technologies such as encryption or web anonymisers [JRC].

A number of **P3P Privacy Tools** are available online such as:

- AT&T P3P Proposal Generator - this tool helps Web site administrators generate P3P "proposals" and corresponding human-readable privacy policies. http://www.research.att.com/projects/p3p/propgen
- Privacy Minder - AT&T Research has developed a P3P user agent implementation called Privacy Minder. Privacy Minder is a client-side proxy designed to be installed on a user's Windows 95/98/NT computer and work with the user's existing Web browser. http://www.research.att.com/projects/p3p/pm
- IBM's P3P Parser - a java package containing classes and methods for parsing, generating, manipulating and evaluating P3P proposals and responses; also contains a parser and evaluator for "A P3P Preference Exchange Language" (APPEL). http://www.alphaworks.ibm.com/formula/p3p
- Privacy Information Management System from the Japanese Electronic Network Consortium. An online tool that enables Website developers to create easily P3P policies compliant with the P3P 1.0 Candidate Recommendation (December 2000). http://www.nmda.or.jp/enc/privacy/eindex.html
- NEC P3P4P Implementation - P3P for Perl library. NEC has made its prototype implementation of a P3P working draft available under the Perl Artistic License. http://www.w3.org/P3P/contributed/nec.co.jp/

Digital watermarking and **watercasting** provide the means for incidents of copying and editing of multimedia data to be traced, if transmitted data are marked using these techniques [Brown, Craver]. Copied multimedia data, once identified, could be traced back to its origins. Sessions could be transmitted with an embedded mark that allows broadcasters to trace their multimedia used publicly elsewhere with a webcrawler-type search engine [Adams-b, Memon].

The Present: Current Projects

GUIDES: Guidelines for Assessing Technological Compliance with the Data Protection Directive. http://dsa-isis.jrc.it/Privacy/GUIDES.html

The aim of the twelve month GUIDES project is to develop a set of guidelines for assessing the privacy compliance of online information systems with regard to the EU Data Protection Directives 95/46/EC & 97/66/EC (DPD).

The development of the world-wide-web and browser based technologies (e.g. HTML, Java, SSL) has created new mechanisms for the implementation of data processing systems over the Internet. These mechanisms are underpinning the rapid developments in the areas of e-commerce, online databases and information management systems. However, there are serious concerns being raised in regard to the abuse of basic privacy principles that is occurring through the use of online systems. The GUIDES project will use case study analysis of typical WWW information processing systems in the areas of e-commerce, health and m-commerce in order to characterise the internet based data handling practices, particularly those pertinent to personal data. Subsequently, these practices will be assessed within the context of the principles for privacy protection defined within the DPDs. The mechanisms that are being used to exploit personal and private data will be analysed and categorised in relation to the EU DPD. In addition, the mechanisms, that are being developed or proposed to support the implementation of privacy principles, particularly technologies such as P3P, digital signatures and anonymous agents, will be assessed to identify how closely they satisfy the requirements of the DPDs.

The outcome of the project will be the production of a set of guidelines that clearly elaborate on the privacy issues relevant to current data processing practices based upon Internet and WWW technologies.

PISA: Privacy Incorporated Software Agent – Proposal for Building a Privacy Guardian for the Electronic Age.

http://pet-pisa.openspace.nl/pisa_org/pisa/pisa_project.html

The challenge is to design a PET-agent, which independently performs miscellaneous tasks online, while fully preserving the privacy of the persons involved, or at least up to the level specified by the persons themselves. The agent should for that purpose be able to distinguish what information should be exchanged under what circumstances to which party. The challenge here is to implement privacy laws, specifically the European Directive 95/46/EC (being the highest privacy standard at this moment in the world) and other rules into specifications for a product. Next the specifications have to be implemented by software programming. Also there should be appropriate (cryptographic) protection mechanisms to ensure the security of the data and prevent 'leakage' to third parties. PET-agents (PISA) will enable the user in its quality of consumer or citizen in e-commerce and e-government transactions and communications to protect himself against loss of his informational privacy contrary to systems like P3P where an asymmetric situation exists to the benefit of the web site owner. PISA empowers the consumer and citizen to decide at any time and under any circumstance when to reveal his or her identity.

The Privacy Incorporate Software Agent (PISA) project aims to build a privacy guardian for the electronic age by:

- Demonstrating Privacy Enhancing Technologies (PET) as a secure technical solution to protecting the privacy of the citizen when he/she is using Intelligent Agents (called shopbots, buybots, pricebots or just "bots", a short for robot) in E-commerce or M-commerce applications, according to EC-Directives on Privacy.
- Interacting with industry and government to launch new privacy protected services.
- Proposing a new open standard for Privacy Protected Agent Transactions to Standardisation Bodies.

The PISA demonstration model is planned to be a novel piece of software that incorporates several advanced technologies in one product:

- Agent technology, for intelligent search and matching ;
- Data mining or comparable techniques to construct profiles and make predictions;

- Cryptography for the protection of personal data, as well as the confidentiality of transactions.

Scenarios for PETs usage

Hes and Borking describe several scenarios that require privacy protection and are suitable for PETs support.

Telecommunications

A digital telephone network enables the receiving party to identify the caller via the telephone number: the network communicates the number to his telephone or other peripheral equipment. This number can be directly displayed or used as a search key within a database so that other data pertaining to the caller are retrieved. This function is knows as Calling Line Identification (CLI).

To date, the service-provider (i.e. a telephone company) still requires the caller's identity in order to charge him for the services provided. This means it is not (yet) possible for the caller to remain anonymous to the service-provider. The person receiving the call is another user of the information system who can be approached via the service of phoning.

The caller can keep his identity secret through the use of an identity protector, which consists of a number of blocking options integrated in the functionality of the Calling Line Identification. In CLI, the caller can determine whether his telephone number is to be revealed. CLI thus offers the functionality of an identity protector. Here, the identity protector is located between the service-provider and the services.

Health Sector

Every day, medical data concerning individuals are stored in databases. Medical information is not only important and interesting to the physician who treats the patient, but to many others like fellow doctors, nursing staff, pharmacists, insurance companies, scientific researchers, and employers. Databases where this information is filed often lack features to protect privacy, meaning that anyone who has access to these databases has access to all data on an individual patient.

Not all involved parties need to know the patient's identity. Scientists conducting research into certain illnesses/trends, for example, do not need to know the identity of the person. What is important to them is that they have access to all the data relevant to a study. Not only the illnesses and treatments that a patient has gone through are of interest, but also certain habits, like smoking, exercise, etc. So far, scientists have used patients' identities in order to collate all of the registered information.

Retail

Users can pay for articles purchased in a store in a number of ways: with cash, with a bankcard, or with a credit card. The last two payment options involve use of data that can easily be linked with the user's identity. The bank statements the shopkeeper receives state highly identifying data, such as the account number and name of the user. If a user wants to remain anonymous, he is currently forced to use the first means of payment, i.e. cash.

The Future: "Enhancing" PETs

Goldberg et al, provide some suggestions for future PETs. "Where the cooperation of others is necessary to ensure personal privacy, the system should not be easily subverted by the mere collusion or compromise of a few participants" [Goldberg]. There is the need for a variety of means by which users can protect their privacy, preferably by putting Privacy Enhancing Technology into their own hands.

So far in this review several Privacy Enhancing Technologies are discussed. It is obvious that more effort in the previous years was invested in protecting user identities rather than personal data. This is partly because of the ongoing debate about personal and sensitive information, but mainly because it was relatively straightforward for research fields such as cryptography to find application domains. There is evidence that more effort is needed especially with P3Ps in order to address issues such as:

- The coverage of privacy needs – practices relating to data collection, limitations on use and disclosure, openness of acquired information, data quality, subject access to data and accountability.

- The coverage of legal and cultural diversity – the P3P team was dominated by American contributors.
- The drivers for implementation - For P3P to have its intended impact, developers need to achieve compliance in new versions of their web-browsers, and to fit the feature into existing versions. Pioneer and early adopted web-site managers, and web-users, need to acquire and apply P3P-compliant software, and to express their practices and their preferences.
- The mechanisms for ensuring compliance - User empowerment is not by itself sufficient, because there is an enormous power imbalance between corporations and individuals.

Finally there is the need for a formal specification of requirements for the next generation of privacy enhancing technologies. A Common Position of the International Working Group on Data Protection in Telecommunications on "Essentials for Privacy Enhancing Technologies on the World Wide Web" suggests "to set out essential conditions that should be met by any technical platform for privacy protection on the World Wide Web with the objective of avoiding a systematic collection of personal data".

References

Adams-a, A. and M.A. Sasse, “Privacy in Multimedia Communications: Protecting Users, Not Just Data”, in Blandford, A., Vanderdonkt, J. and P. Gray (Eds.), “People and Computers XV – Interaction Without Frontiers, Joint Proceedings of HCI 2001 and ICM 2001, Lille, September 2001, pp 49-64, Springer.

Adams-b, A. and M.A. Sasse, “Taming the Wolf in Sheep’s Clothing: Privacy in Multimedia Communications”, Proceedings of ACM Multimedia ’99, Orlando, Florida, November, 1999, pp 101-107.

Blaze, M., Feigenbaum, J. and J. Lacy, “Decentralised Trust Management”, Proceedings of the IEEE Symposium on Security and Privacy, Oakland, 1996, pp 164-173 ftp://dimacs.rutgers.edu/pub/dimacs/TechnicalReports/TechReports/1996/96-17.ps.gz

Brown, I., C. Perkins and J. Crowcroft, “Watercasting: Distributed Watermarking of Multicast Media”, Globecom ’99, Rio de Janeiro, December, 1999.

Burkert, H., “Privacy Enhancing Technologies: Typology, Vision, Critique” in Agre, P.E. and M. Rotenberg (Eds.), “Technology and Privacy: The New Landscape”, ISBN 0-262-01162-X, MIT Press, 1997.

Chaum-a, D. “Showing Credentials without Identification Transferring Signatures Between Unconditionally Unlinkable Pseudonyms”, Advances in Cryptology in AUSCRYPT ’90, January 1990, pp 246-264.

Chaum-b, D., “Untraceable Electronic Mail, Return addresses, and Digital Pseudonyms”, Communications of the ACM, February 1981, vol. 24 no. 2. http://www.eskimo.com/~weidai/mix-net.txt

Chaum-c, D., “Blind Signatures for Untraceable Payments”,' *CRYPTO 82*, Plenum, pp. 199-203.

Chu, Y.H., Feigenbaum, J. LeMacchia, B. Resnick, P. and M. Strauss, "REFEREE: Trust Management for Web Applications, 1997 http://w3j.com/7/s3.referee.wrap.html

Cotrell, L., "Mixmaster & Remailer Attacks", 1995 http://www.obscura.com/~loki/remailer/remailer-essay.html

Craver, S., B. Yeo and M. Yeung, "Technical Trials and Legal Tribulations", Communications, ACM, 41, 7, pp 45-54, 1998.

Hes, R. and J. Borking, "Privacy Enhancing Technologies: The Path to Anonymity", Background Studies and Investigations, 1998 http://www.registratiekamer.nl/bis/top-1-11.html

Clarke, R., "Roger Clarke's PITs and PETs Resources Site", http://www.anu.edu.au/people/Roger.Clarke/DV/PITsPETsRes.html

Fischer-Hubner, S. "Privacy Enhancing Technologies DAV D18", Karlstad University, Department of Computer Science, PhD Course, Lecture Notes, Sessions 1-11, http://www.cs.kau.se/~simone/kau-phd-course.htm

Goldberg, I., Wagner, D. and E. Brewer, "Privacy-Enhancing Technologies for the Internet", IEEE COMPCON '97, http://www.cs.berkeley.edu/~daw/papers/privacy-compcon97-www/privacy-html.html

Jackson, T. and A. Servida, "The Role of Technology in Facilitating On-Line Privacy", Workshop Report, Joint Research Centre, 2000, http://das-isis.jrc.it/Privacy

Linn, J., "Privacy Enhancement for Internet Electronic Mail: Part I - Message Encipherment and Authentication Procedures", Network Working Group, DEC, IAB, Privacy Task Force August 1989 ftp://ftp.isi.edu/in-notes/rfc1113.txt

Kohntopp, M. and I. Ruhmann, "Trust through Participation of Trusted Parties in Technology Design", Miller, G. and K. Rannenberg (Hg) Multilateral Security in Communications – Technology, Infrastructure, Economy, Proceedings Multilateral

Security in Communications, July 16-17, 1999, Stuttgart, Addison-Wesley-Longman, Munchen, 1999, pp 499-514.

Memon, N. and P.W. Wong, "Protecting Digital Media Content", Communications of the ACM, 41, 7, July, 1998.

Nilsson, M., Lindskog, H. and S. Fischer-Hubner, "Privacy Enhancement in the Mobile Internet", in Proceedings of the IFIP WG 9.6/11.7 Working Conference on Security and Control of IT in Society, Bratislava, June 15-16, 2001, ISBN 3-901882-13-8.

Sottong-Micas, C. and U. Hillbrand, "Data Protection: Privacy Enhancing Technologies – Looking for Concrete Answers", Internal Market, Single Market News No 19, December 1999,
http://www.europa.eu.int/comm/internal_market/en/smn/smn19/s19mn29.htm

Bibliography

Agre, P.E. and M. Rotenberg (Eds.), "Technology and Privacy: The New Landscape", ISBN 0-262-01162-X, MIT Press, 1997.

Federrath, H. (Ed.), "Designing Privacy Enhancing Technologies", LNCS 2009, ISBN 3-540-41724-9, Springer, 2001.

Fischer-Hubner, S. "IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms", LNCS 1958, ISBN 3-540-42142-4, Springer, 2001.

Garfinkel, S. and G. Spafford, "Privacy-Protecting Technologies", Chapter 10 in Web Security, Privacy & Commerce: Security for Users, Administrators & ISPs, 2nd edition, O'Reilly, 2002.

Research Groups, Projects & On Line Resources

College Bescherming Persoonsgegevens (CBP), Dutch Data Protection Authority http://www.registratiekamer.nl

The Privacy Hub: Joint Research Centre (JRC) Institute for Systems, Informatics and Safety (ISIS), European Commission
http://dsa-isis.jrc.it/Privacy/

The Platform for Privacy Preferences Project (P3P) http://www.w3.org/P3P/
International Working Group on Data Protection in Telecommunications, http://wwww.datenschutz-berlin.de/doc/int/iwgdpt/priv_en.htm

++

SEMPER: Secure Electronic Marketplace for Europe - Development of a generic architecture for secure electronic commerce over networks, in particular the Internet. http://www.semper.org/

JEDI-FIRE: Jedi flexible electronic commerce firewall and data privacy - Development of a secure system to support high-speed electronic-commerce applications. http://www.cordis.lu/esprit/src/omi25530.htm

SCAN: Secure Communication in ATM Networks - Confidential communication in asynchronous transfer mode (ATM) networks.
http://www.infowin.org/ACTS/RUS/PROJECTS/ac330.htm

SCARAB: Smart Card and Agent enabled Reliable Access - Smart card technology for distributed and secure telecommunication service architectures.
http://www.infowin.org/ACTS/RUS/PROJECTS/ac339.htm

TRADE: Trials in the Domain of Electronic Commerce - Evaluation of secure multimedia Electronic Commerce platforms for residential and business users. http://www.infowin.org/ACTS/RUS/PROJECTS/ac328.htm

ICE-TEL: Interworking Public Key Certification Infrastructure for Europe - Development of public key-based security in WWW applications. http://www.darmstadt.gmd.de/ice-tel

TIE: Trust Infrastructure for Europe - Development of an infrastructure to support Electronic Commerce in Europe.
http://www.ispo.cec.be/Ecommerce/books/aecev2/2_6.htm

ICE-CAR: Interworking Public Key Certification Infrastructure for Commerce, Administration and Research - Development of European security technology for the purpose of securing open networks. http://ice-car.darmstadt.gmd.de/

E-CLIP: Electronic Commerce Legal Issues Platform - Promotion of awareness regarding legal issues of electronic commerce, particularly among SMEs and sire developers. http://www.jura.uni-muenster.de/eclip/

DAPRO: Data Protection in the European Union - Development of an information server to expound the content of the July 1995 EU Data Protection Directive as a basis for legal regulation of expanding telematics applications, and to clarify its relation to Member State law. http://www.dapro.uni-hanover.de/

ICX: International Commerce Exchange - Development of Codes of Conduct supporting data protection directive principles in business.
http://www.icx.org/home/homeframe.htm

++

http://www.adsubtract.com
http://www.junkbuster.com
http://www.freedom.net
http://www.symantec.com/sabu/nis/nis_pe/
http://www.webwasher.com
http://www.anonymizer.com

http://www.hushmail.com

http://www.omniva.com

Events

The Role of Technology in Facilitating On-Line Privacy: A Workshop for Identifying Technology Requirements to Support EU Data Protection Legislation, Centre Albert Borchette, Brussels, May 17, 2000.

Workshop on Privacy Enhancing Technologies and Privacy Practices, Brussels, Belgium, June 5, 2001, Organised by EICTA: European Information and Communications Technology Industry Association.

Workshop on Design Issues in Anonymity and Unobservability 2000, Berkeley, CA, USA, July 25-26, 2000, Proceedings: Lecture Notes in Computer Science 2009 Springer 2001, ISBN 3-540-41724-9, Hannes Federrath (Ed.).

PET 2002: Workshop on Privacy Enhancing Technologies, Cathedral Hill Hotel, San Francisco, CA, USA, April 14-15, 2002.

Trust and Privacy in Digital Business, http://www.wi-inf.uni-essen.de/~trustbus02/, 13th Conference on Database and Expert Systems Applications (DEXA'02) http://www.dexa.org/dexa02, to be held in Aix-en-Provence, France, Sept 2-6, 2002