



Data Protection Technical Guidance Note:

Privacy enhancing technologies (PETs)

This technical note is intended to raise awareness of the concept of privacy enhancing technologies and is aimed at system designers and those commissioning them. It will give a brief description of privacy enhancing technologies but draws on the extensive information published elsewhere. It is not intended to be an exhaustive account; rather it is a point of entry for readers to further their own research.

Background

Individuals' use of the internet and email to communicate, research areas of interest and interact with businesses and government is at an all time high driven by the strong uptake of broadband services in the UK. At the same time the UK government and devolved administrations are committed to maximising the electronic interaction between the individual and the state at all levels and to sharing information across the databases that authorities control.

There is a growing move towards introducing computing power and/or information storage in everyday consumer products, which will redefine how we interact with our surroundings and could potentially generate information about the opinions, preferences and lifestyles of individuals at an as yet unknown level.

What are privacy enhancing technologies?

Technology can assist companies' compliance with the principles that protect individuals' privacy and can go further to empower individuals, giving them easier access to and control over information about them and allowing them to decide how and when it will be disclosed to and used by third parties.

The best protection for individuals is that their personal information is only collected where this is essential. Privacy enhancing technologies have traditionally been limited to 'pseudonymisation tools'. These are software and systems that allow individuals to withhold their true identity from those operating electronic systems or providing services through them, and only reveal it when absolutely necessary. These technologies help to minimise the information collected about individuals and include anonymous web browsers, specialist email services, and digital cash.

Federated identity management systems potentially allow individuals to access the services of organisations without having to provide information to them. They involve one trusted organisation verifying the identity of an individual and then vouching for them using an electronic token that also

specifies their particular entitlements. This allows the individual to access the services provided by third parties using the token without having to disclose their identity or other information necessary to prove their entitlement.

The Information Commissioner considers that privacy enhancing technologies are not limited to tools that provide a degree of anonymity for individuals but they are also any technology that exists to protect or enhance an individual's privacy, including facilitating individuals' access to their rights under the Data Protection Act 1998.

Examples of this wider approach to privacy enhancing technologies could include:

- encrypted biometric access systems that allow the use of a fingerprint to authenticate an individual's identity, but do not retain the actual fingerprint;
- secure online access for individuals to their own personal data to check its accuracy and make amendments;
- software that allows browsers to automatically detect the privacy policy of websites and compares it to the preferences expressed by the user, highlighting any clashes; and
- 'sticky' electronic privacy policies that are attached to the information itself preventing it being used in any way that is not compatible with that policy.

Why use privacy enhancing technologies?

They can save you money. The cost of including privacy at the system design stage is much less than the cost of having to amend a finished system to make sure it complies with legal requirements and respects individuals' privacy.

They help to reduce risks. Privacy controls that are incorporated into electronic information systems to supplement organisational procedures help to provide additional safeguards which better protect individuals' information from human error.

They help to build trust. The use of privacy enhancing technology in systems helps to signal the integrity and intention of organisations regarding the information that they hold, and encourages trust in those organisations by citizens and customers.

The design philosophy

A system designer who starts from the position of trying to protect individuals' privacy by creating or implementing privacy enhancing technologies might ask the following questions as an essential part of the task.

- Do I need to collect any personal data at all?

- If so, what is the minimum needed?
- Who will have access to which data?
- How can accesses be controlled to allow only those which are for the purposes stated when the data was collected, and then only by those employees and processes that have an essential need?
- Can individuals make total or partial use of the system anonymously?
- How can I help individuals to exercise their rights securely?

In 2003, the HiSPEC team at the University of Manchester Institute of Science and Technology produced data protection best practice guidance for system designers in collaboration with the Information Commissioner's Office, which can be found on their website (see below).

Useful information sources

Data protection and privacy commissioners

Ontario data protection authority

Privacy enhancing technology testing and evaluation project (PETTEP) documentation

http://www.ipc.on.ca/scripts/index.asp?action=31&N_ID=1&P_ID=15495&U_ID=0

Dutch data protection authority

Privacy enhancing technologies – a white paper for decision makers

http://www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf?refer=true&theme=purple

Privacy-Enhancing Technologies – the path to anonymity. Revised edition (1998)

http://www.dutchdpa.nl/documenten/EN_av_11_Privacy-enhancing_technologies.shtml

Researchers and academics

Rand Europe

Technology solutions to protect privacy in e-government

<http://www.rand.org/randeurope/review/2.3-horlings.html>

Roger Clarke

Introducing PITs and PETS Technologies: technologies affecting privacy

<http://www.anu.edu.au/people/Roger.Clarke/DV/PITsPETS.html>

UMIST

Data protection best practice guidance

http://www.hispec.org.uk/public_documents/BPDMay02.pdf

Privacy enhancing technologies state of the art review (2002)

http://www.hispec.org.uk/public_documents/7_1PETreview3.pdf

Conferences

The workshop on privacy enhancing technologies

<http://petworkshop.org/2006/index.htm>

More information

If you need any more information about this or any other aspect of data protection, please contact us.

Phone: 01625 545745

Email: mail@ico.gsi.gov.uk

Website: www.ico.gov.uk