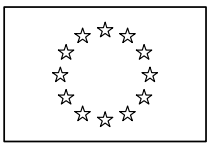

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 2.5.2007
COM(2007) 228 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on Promoting Data Protection by Privacy Enhancing Technologies (PETs)

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on Promoting Data Protection by Privacy Enhancing Technologies (PETs)

(Text with EEA relevance)

1. INTRODUCTION

The intensive and sustained development of information and communication technologies (ICT) is constantly offering new services which improve people's life. To a large extent, the raw material for interactions in cyberspace is the personal data of individuals moving around in it when they purchase goods and services, establish or maintain contact with others or communicate their ideas on the world wide web. Alongside the benefits brought about by these developments, new risks also arise for the individual, such as identity theft, discriminatory profiling, continuous surveillance or fraud.

The Charter of Fundamental Rights of the European Union recognises in Article 8 the right to the protection of personal data. This fundamental right is set forth in a European legal framework on the protection of personal data consisting in particular of the Data Protection Directive 95/46/EC[1] and the ePrivacy Directive 2002/58/EC[2] as well as the Data Protection Regulation (EC) 45/2001[3] relating to processing by Community institution and bodies. This legislation lays down several substantive provisions imposing obligations on data controllers and recognizing rights of data subjects. It also prescribes sanctions and appropriate remedies in cases of breach and establishes enforcement mechanisms to make them effective.

However, this system may prove insufficient when personal data is disseminated worldwide through ICT networks and the processing of data crosses several jurisdictions, often outside the EU. In such situations the current rules may be considered to apply and to provide a clear legal response. Furthermore, a competent authority to enforce the rules may also be identified. However, considerable practical obstacles may exist as a result of difficulties with the technology used involving data processing by different actors in different locations and there may be hurdles intrinsic to the enforcement of national administrative and court rulings in another jurisdiction, especially in non-EU countries.

Whilst strictly speaking data controllers bear the legal responsibility for complying with data protection rules, others also bear some responsibility for data protection from a societal and

---

1 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31.

2 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.07.2002, p. 37.

3 Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p. 1-22.

ethical point of view. These involve those who design technical specifications and those who actually build or implement applications or operating systems.

Article 17 of the Data Protection Directive lays down the data controller's obligation to implement appropriate technical and organisational measures and to ensure a level of security appropriate to the nature of the data and the risks of processing it. The use of technology to support the respect for legislation, in particular the data protection rules, is already envisaged to some extent in the ePrivacy Directive[4].

A further step to pursue the aim of the legal framework, whose objective is to minimise the processing of personal data and using anonymous or pseudonymous data where possible, could be supported by measures called Privacy Enhancing Technologies or PETs - that would facilitate ensuring that breaches of the data protection rules and violations of individual's rights are not only something forbidden and subject to sanctions, but technically more difficult.

The purpose of this Communication, which follows from the First Report on the implementation of the Data Protection Directive[5], is to consider the benefits of PETs, lay down the Commission's objectives in this field to promote these technologies, and set out clear actions to achieve this goal by supporting the development of PETs and their use by data controllers and consumers.

2. WHAT ARE PETS?

There are a number of definitions of PETs used by the academic community and by pilot projects on this matter. For instance, according to the EC-funded PISA project, PET stands for 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 information system. The use of PETs can help to design information and communication systems and services in a way that minimises the collection and use of personal data and facilitate compliance with data protection rules. The Commission in its First Report on the implementation of the Data Protection Directive considers that *"...the use of appropriate technological measures is an essential complement to legal means and should be an integral part in any efforts to achieve a sufficient level of privacy protection..."*. The use of PETs should result in making breaches of certain data protection rules more difficult and/or helping to detect them.

In the dynamic landscape of ICT, the effectiveness of different PETs to ensure the protection of privacy, including aspects of compliance with data protection law, is varied and changes over time. Their typology is also varied. They can be stand-alone tools requiring positive action by consumers (who must purchase and install them in their PCs) or be built into the very architecture of information systems. Several examples of PETs can be mentioned here:

- Automatic anonymisation of data, after a certain lapse of time, supports the principle that processed data should be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the data were originally collected.

---

4 Recital 46 and Article 14(3) of Directive 2002/58/EC

5 COM (2003) 265(01), 15.5.2003, see http://eurlex.europa.eu/LexUriServ/site/en/com/2003/com2003_0265en01.pdf

- Encryption tools, preventing hacking when information is transmitted over the Internet, supports the data controller's obligation to take appropriate measures to protect personal data against unlawful processing.

- Cookie-cutters, that block cookies placed on the user's PC to make it perform certain instructions without the user being aware of them, enhance compliance with the principle that data must be processed fairly and lawfully, and that the data subject must be informed about the processing going on.

- The Platform for Privacy Preferences (P3P), allowing internet users to analyze the privacy policies of websites and compare them with the user's preferences as to the information they wish to release, helps to ensure that data subjects' consent to processing of their data is an informed one.

3. THE COMMISSION SUPPORTS PETS

The Commission considers that PETs should be developed and more widely used, in particular where personal data is processed through ICT networks. The Commission considers that wider use of PETs would improve the protection of privacy as well as help fulfil data protection rules. The use of PETs would be complementary to the existing legal framework and enforcement mechanisms.

In its Communication on a strategy for a secure Information Society, COM(2006) 251 of 31 May 2006, the Commission invited in particular the private sector to "*stimulate the deployment of security-enhancing products, processes and services to prevent and fight ID theft and other privacy-intrusive attacks*". Furthermore, in the Commission's Roadmap for a pan-European eIDM Framework by 2010[6] one of the key principles governing electronic identity management is that *"the system must be secure, implement the necessary safeguards to protect the user's privacy, and allow its usage to be aligned with local interest and sensitivities"*.

The intervention of different actors in data processing and the existence of different national jurisdictions involved could make enforcement of the legal framework difficult. On the other hand, PETs could ensure that certain breaches of data protection rules, resulting in invasions of fundamental rights including privacy, could be avoided because they would become technologically more difficult to carry out. The Commission is aware of the fact that technology – although having a crucial role in privacy protection – is not sufficient in itself to secure privacy. PETs need to be applied according to a regulatory framework of enforceable data protection rules providing a number of negotiable levels of privacy protection for all individuals. The use of PETs does not mean that operators can be discharged of certain of their legal obligations (e.g. granting individual users a right of access to their data).

Important public interests could also be better served. The data protection legal framework provides for restrictions to the general principles and interference in the rights of individuals for important public interests such as public security, the fight against crime or public health. The conditions for such restrictions are laid down in Article 13 of the Data Protection Directive and Article 15 of the ePrivacy Directive. They are substantially similar to those set

[6] http://ec.europa.eu/information_society/activities/egovernment_research/doc/eidm_roadmap_paper.pdf

by Article 8 of the European Convention on Human Rights (ECHR), namely that such interference is done in accordance with the law and is proportionate and necessary in a democratic society for a legitimate public purpose[7]. The use of PETs should not prevent law enforcement agencies or other competent authorities from intervening in the lawful exercise of their functions for an important public interest, e.g. fighting cybercrime, combating terrorism or preventing the spread of contagious diseases. The responsible authorities should be in a position to access personal data where necessary to achieve those purposes and in accordance with the procedures, conditions and safeguards laid down by the law.

Better respect of data protection rules would also have a positive impact on consumer trust, in particular in cyberspace. A number of promising and value-added services that rely on transfers of personal data across IT-Networks, such as e-learning, e-government, e-health, e-banking, e-commerce or "intelligent car" systems would certainly benefit. People could be sure that the data they are providing to identify themselves, receive services or make payments will only be used for legitimate purposes and that their participation in the digital community is not done at the expense of sacrificing their rights.

4. WORK DONE AND THE WAY FORWARD

To pursue the objective of enhancing the level of privacy and data protection in the Community by, among others, promoting the development and the use of PETs, the Commission intends to conduct the following activities, involving a vast array of actors, including its own services, national authorities, industry and consumers.

In these discussions attention will be given to the specific situation of small and medium-sized enterprises (SMEs) and the possibilities or incentives for their use of PETs. The Commission should also, among other issues, consider trust and awareness - issues which are of particular importance to SMEs.

4.1. First objective: to support the development of PETs

If PETs are to be widely used, there needs to be further design, development and manufacturing of PETs. Whilst these activities are already done to a certain degree by the public and private sector the Commission considers that these activities should be stepped up. With this aim in mind, the need for PETs and their technological requirements should be identified and RTD activities should develop the tools.

4.1.1. Action 1.1.: Identifying the need and technological requirements of PETs

PETs are heavily dependent on the evolution of ICT. Once the dangers posed by technological developments are detected, the appropriate requirements for a technological solution must be identified.

The Commission will encourage various stakeholder groups to come together and debate PETs. These groups will include in particular representatives from the ICT sector, PETs developers, data protection authorities, law enforcement bodies, technology partners including experts from relevant fields, such as eHealth or information security, consumers and civil

[7] European Court of Justice, judgment of 20.5.2003, Joined cases C-465/00, C-138/01 and C-139/01 "Österreichischer Rundfunk and Others" ("Rechnungshof") ECR [2003] I-04989, paragraphs 71 and 72.

rights associations. These stakeholders should regularly look into the evolution of technology, detect the dangers it poses to fundamental rights and data protection, and outline the technical requirements of a PETs response. .This may include fine-tuning the technological measures in accordance with the different risks and the different data at stake and taking into account the need to safeguard public interests, such as public security.

4.1.2. Action 1.2.: Developing PETs

As the need for and technological requirements of PETs are identified, concrete action has to be taken to arrive at an end-product ready to use.

The Commission has already addressed the need for PETs. Under the auspices of the 6th Framework Programme it sponsors the PRIME[8] project tackling issues of digital identity management and privacy in the information society. The OPEN-TC[9] project will allow privacy protection based on open trusted computing and the DISCREET[10] project develops middleware to enforce privacy in advanced network services. In the future, under the 7th Framework Programme, the Commission intends to support other RTD projects and large-scale pilot demonstrations to develop and stimulate the uptake of PETs. The aim is to provide the foundation for user-empowering privacy protection services reconciling legal and technical differences across Europe through public-private partnerships.

The Commission also calls on national authorities and on the private sector to invest in the development of PETs. Such investment is key to placing European industry ahead in a sector that will grow as these technologies become increasingly required by technological standards and by consumers more aware of the need to protect their rights in cyberspace.

4.2. Second objective: to support the use of available PETs by data controllers

PETs will only be truly beneficial if they are effectively incorporated into and used by technical equipment and software tools that carry out processing of personal data. The participation of the industry that manufactures such equipment and of data controllers who avail themselves of it to carry out data processing activities is therefore paramount.

4.2.1. Action 2.1.: Promoting the use of PETs by industry

The Commission believes that all those involved in processing of personal data would benefit from a wider use of PETs. The ICT industry, as the primary developer and provider of PETs, has a particularly important role to play with respect to the promotion of PETs. The Commission calls on all data controllers to more widely and intensely incorporate and apply PETs in their processes. For that purpose, the Commission will organise seminars with key actors of the ICT industry, and in particular PETs developers, with the aim of analyzing their possible contribution to promoting the use of PETs among data controllers.

The Commission will also conduct a study on the economic benefits of PETs and disseminate its results in order to encourage enterprises, in particular SMEs, to use them.

---

8 https://www.prime-project.eu/
9 http://www.opentc.net/
10 http://www.ist-discreet.org/

4.2.2. Action 2.2.: Ensuring respect for appropriate standards in the protection of personal data through PETs

While wide-reaching promotional activity requires the active involvement of the ICT industry, as the PETs producer, respect for appropriate standards requires action beyond self-regulation or the goodwill of the actors involved. The Commission will assess the need to develop standards regarding the lawful processing of personal data with PETs through appropriate impact assessments. On the basis of the outcome of such assessments, two sorts of instruments might be considered:

- *Action 2.2.a) Standardisation*

The Commission will consider the need for respect of data protection rules to be taken into account in standardisation activities. The Commission will endeavour to take account of the input of the multi-stakeholder debate on PETs in preparing the corresponding Commission actions and the work of the European standardisation bodies. This will be paramount, in particular, where the debate identifies appropriate data protection standards requiring the incorporation and use of certain PETs.

The Commission may invite the European Standardisation Organisations (CEN, CENELEC, ETSI) to assess specific European needs, and to subsequently bring them to the international level by means of applying the current agreements between European and international standardisation organisations. Where appropriate, the ESOs should establish a specific standardisation work programme covering European needs and thus complementing the on-going work at international level.

- *Action 2.2.b) Coordination of national technical rules on security measures for data processing*

National legislation adopted pursuant to the Data Protection Directive[11] gives national data protection authorities certain influence in determining precise technical requirements such as providing guidance for controllers, examining the systems put in place or issuing technical instructions. National data protection authorities could also require the incorporation and use of certain PETs where the processing of personal data involved makes them necessary. The Commission considers that this is an area where coordination of national practice could contribute positively to promoting the use of PETs. In particular the Article 29 Working Party[12] could contribute in its role of considering the uniform application of national measures adopted under the Directive. The Commission thus calls on the Article 29 Working Party to continue its work in the field by including in its programme a permanent activity of analysing the needs for incorporating PETs in data processing operations as an effective means of ensuring respect for data protection rules. This work should then produce guidelines for data protection authorities to implement at national level through coordinated adoption of the appropriate instruments.

---

[11] e.g. Article 17

[12] Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up by Article 29 of Directive 95/46/EC.

4.2.3. Action 2.3.: Promoting the use of PETs by public authorities

A consistent number of processing operations involving personal data are conducted by public authorities in the exercise of their competences, both at national and at Community level. Public bodies are themselves bound to respect fundamental rights, including the right to protect personal data, and ensure respect by others, and should therefore set a clear example.

As regards national authorities, the Commission notes the proliferation of eGoverment applications as a tool for enhancing effectiveness of public service. As stated in the *Commission's Communication on the Role of eGoverment for Europe's Future*[13], the use of PETs in eGovernment is necessary to provide trust and confidence to ensure its success. The Commission calls upon governments to ensure that data protection safeguards are embedded in eGovernment applications, including through the widest possible use of PETs in their design and implementation.

As for Community institutions and bodies, the Commission itself will ensure that it complies with the requirements of Regulation (EC) 45/2001 in particular through a wider use of PETs in the implementation of ICT applications involving the processing of personal data. At the same time, the Commission calls on other EU institutions to do the same. The European Data Protection Supervisor could contribute with his advice to Community institutions and bodies on drawing up internal rules relating to the processing of personal data. When selecting new ICT applications for its own use, or when developing existing applications, the Commission will consider the possibility of introducing privacy enhancing technologies. The importance of PETs will be reflected in the Commissions' overall IT governance strategy. The Commission will also continue to raise awareness in its own staff. However, the implementation of PETs in the Commissions' ICT applications depends on the availability of the corresponding products and will have to be evaluated on a case by case basis, in line with the application's development cycle.

4.3. Third objective: to encourage consumers to use PETs

Consumers will remain the most concerned party in ensuring personal information is properly used, that data protection rules are properly enacted, and that PETs are an efficient means to guarantee them.

Consumers should therefore be made fully aware of the advantages that the use of PETs may bring to diminish the risks posed by operations involving processing of their personal data. They should also be placed in a position where they may exercise an informed choice when purchasing IT equipment and software, or using e-services. This should reflect their awareness of the risks involved, in particular whether PETs offer appropriate protection. Simple and understandable information about possible technological tools to protect privacy must thus be provided to the user. Increased use of PETs and increased use of e-services which incorporate PETs will in turn mean economic reward to the industries using them, and may result in a snowball effect, encouraging other companies to pay greater attention to respecting the data protection rules. In order to achieve this, a series of steps should be taken.

---

[13] COM (2003) 567 final, 26.9.2003.

4.3.1. Action 3.1.: Raising awareness of consumers

A consistent strategy should be adopted to raise consumer awareness of the risks involved in processing their data and of the solutions that PETs may provide as a complement to the existing systems of remedies contained in data protection legislation. The Commission intends to launch a series of EU-wide awareness-raising activities on PETs.

The main responsibility for conducting this activity falls within the realm of national data protection authorities which already have relevant experience in this area. The Commission calls on them to increase their awareness-raising activities to include information on PETs through all possible means within their reach. The Commission also urges the Article 29 Working Party to coordinate national practice in a coherent work plan for awareness-raising on PETs and to serve as a meeting point for the sharing of good practice already in place at national level. In particular, consumer associations and other players such as the Consumer Centres Network (ECC-Net), in its role as an EU-wide network to advise citizens on their rights as consumers, could become partners in the quest to educate consumers.

4.3.2. Action 3.2.: Facilitating consumers' informed choice: Privacy Seals

The take-up and use of PETs could be encouraged if the presence of these technologies in a certain product and its basic features are easily recognizable. For that purpose, the Commission intends to investigate the feasibility of an EU-wide system of privacy seals, which would also include an economic and societal impact analysis. The purpose of such privacy seals would be to ensure consumers can easily identify a certain product as ensuring or enhancing data protection rules in the processing of data, in particular by incorporating appropriate PETs.

In order for privacy seals to achieve their purpose, the Commission considers that the following principles should be respected:

– The number of privacy seal systems should be kept to a minimum. In fact, a proliferation of seals may create more confusion to the consumer and undermine their trust in all seals. Therefore, an assessment should be made about whether and to what extent it would be appropriate to integrate a European privacy seal in a more general security certification scheme[14].

– Privacy seals should only be awarded for a product's compliance with a set of standards corresponding to data protection rules. The standards should be as uniform as possible throughout the EU.

– Public authorities, in particular national data protection authorities, should play an important role in the system through their involvement in the definition of relevant standards and procedures as well as in monitoring the functioning of the seal system.

With this in mind, and taking account of previous experience concerning seal programmes in other areas (e.g. environment, agriculture, security certification for products and services), the

---

[14] In its Communication of 31 May 2006 on a Strategy for a secure Information Society "Dialogue, partnership and empowerment"(COM (2006) 251 final), the Commission has already invited the private sector to "work towards affordable security certification schemes for products, processes and services that will address EU-specific needs (in particular with respect to privacy)".

Commission will conduct a dialogue with all the stakeholders concerned, including national data protection authorities, industrial and consumer associations and standardisation bodies.