Privacy, Technology, and Europe

A Report for Japan's Ministry of Public Management Home Affairs Postal and Telecommunications

March 2003

Contact: *Privacy International*
http://www.privacyinternational.org/

Contents

Authors and Acknowledgements

The country reports were authored by Ian Brown (UK), Stephan Engberg (Denmark), Herkko Hietanen and Mikko Valimaki (Finland), and Jerome Thorel (France). Wendy M. Grossman provided significant analysis and editing. Simon Davies co-ordinated the research. Gus Hosein was the managing editor of this report.

The editor of this report would like to thank Rigo Wenning (W3C), Michael Waidner (IBM-Zurich research labs), Caspar Bowden (Microsoft Europe), Pete Bramhall (HP Labs-Bristol), Marit Hansen (Independent Centre for Privacy Protection-Kiel) for their remarkable assistance and expertise.

Section I. Privacy in Europe

Introduction

At first sight, the prospects for privacy protection in Europe appear to be bleak, and the outlook for privacy technologies even more so. Scrutiny of the activities and interests of individuals is increasing. Legal protections over personal data are routinely compromised. Information and Communications infrastructures are exhibiting a trend to 'surveillance by design', in which surveillance is established as a core design component of new systems. Global co-operation by law enforcement organisations, national security agencies and technical standards bodies ensures, for example, that all forms of new communication are 'wiretap friendly', and that new mobile technologies are capable of incorporating geographic tracking.

While this situation is without doubt inimical to the development of strong privacy safeguards, it cannot be said that privacy has become obliterated in Europe. Data Protection laws continue to exert a positive influence on the development of information processes. Many organisations already use a plethora of technologies to limit the collection and dissemination of certain classes of data. At its simplest level, for example, technologies used in call centres incorporate safeguards to prevent the misuse or manipulation of personal information held electronically.

While it is true that information systems frequently aid the protection of privacy at these fragmented "front-end" levels, the root data reserves and identification systems of all key sectors of government and private sector invariably rely on "seamless" personal identification supported by a substantial quantity of auxiliary data relating to the individual. At these core levels, the concept of "embedded" privacy has yet to be explored.

There is no doubt that technology always had the potential to play an important role in the protection of privacy even at the core level of administration. The pioneering work of, for example, Erik Boe (Norway) and David Chaum (Netherlands) demonstrated more than a decade ago that privacy and anonymity could be successfully embedded into major national systems. However, these and other researchers have encountered a range of insurmountable problems in promoting their ideas. The key difficulty they encountered is that such concepts as anonymity face an almost pathological resistance amongst many security and administration managers.

It is superficially tempting to suggest a conspiracy against privacy enhancing techniques and technologies. A closer inspection of the facts contained in this report reveals a far more complex set of dynamics. Privacy technologies cannot exist in a vacuum. They must be supported by sympathetic laws and responsive organisational culture. These factors can be shaped by a range of drivers, including public opinion and market dynamics. This necessary convergence at a general level has yet to occur.

While this set of requirements establishes a huge challenge for privacy, it should be noted that an almost identical failure of convergence has inhibited the onset of greater surveillance in Europe. Attempts by authorities to institute repressive surveillance regimes are routinely thwarted because of technological failure, public resistance, financial considerations or constitutional safeguards. The pursuit of privacy and the creation of surveillance exhibit complex and parallel dynamics that are in constant turbulence and change.

Despite these parallel dynamics privacy is disadvantaged because of two primary reasons. First, the concept of embedded surveillance and perfect identity has gained acceptance faster than the concept of embedded privacy and anonymity. Second, governments in charge of large information systems have the luxury of writing the rules. Exemptions in favour of surveillance are written into law on the basis of a stated "public interest", while requirements for the protection of privacy rarely have such a weighty pedigree. Public interest exemptions from data protection laws have resulted in wholesale violations of privacy. The imposition by financial services regulators and insurance companies of statutory and non-statutory reporting and audit requirements creates a further imbalance. While acknowledging the importance of privacy as a fundamental right, data controllers argue that surveillance is necessary to maintain law and order and to create economic efficiency, and that privacy rights in general must remain subject to constraints of fiscal and public interest.

European data protection laws in general, arguably the most advanced in terms of recognising the importance of adequate data protection, have done little to prevent the spread of DNA testing, the use of identity cards, workplace surveillance, police powers, intrusion by tax authorities, Internet snooping and national security surveillance of civilian communications in the countries that comprise the European Union. Unlike other rights such as freedom of expression or freedom of movement privacy in itself is not seen as constituting a public interest.

If the principles of data protection were enforced across the information spectrum (without, for example, broad public interest exemptions), it is feasible that current legislation might create a more supportive environment for the development of privacy technologies. However, there are three addi-

tional factors that prevent this condition from occurring. First, individuals – while consistently expressing anxiety about privacy invasion – are overwhelmed by the processes required to enforce protection of their privacy. Resistance to the use of conventional encryption techniques is one example. Second, privacy and data protection regulators are frequently fatalistic, timid or under-resourced, resulting in management that is based on reaction rather than advocacy. Finally, many protections – whether legal or technological – are frequently undermined by options to discard privacy either through inducement or coercion.

These factors should not induce a fatalistic attitude. As information becomes a more significant part of our lives, and as people become more educated about the risks posed by improper use of data, interest in privacy is likely to escalate. As this interest increases, the motivation at a political and at a marketplace level to promote privacy should also increase.

The current situation in Europe indicates that the environment for embedded privacy protection will not evolve uniformly, but is more likely to develop in a piecemeal fashion. Even with such a fragmented evolution, the existence of such technology, coupled with growing anxiety over surveillance, is likely to help redress the rhetorical imbalance between privacy and surveillance.

Legal Context

Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950 establishes within ratified states the right to privacy:

> *(1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health of morals, or for the protection of the rights and freedoms of others.* [1]

[1] Council of Europe. Convention for the Protection of Human Rights and Fundamental Freedoms, (ETS no: 005). Strasbourg, open for signature November 4, 1950, entry into force September 3, 1950.

Within this very definition we see the strains with which European public policy is currently grappling.

That is, the protection of the right to privacy is paramount, a constitutional right protected by the ECHR. If it were so simple, the regulatory landscape would be clean and clear; and technologies to support this right could be constructed easily. National laws, however, may be created to interfere with this law; much as there are technologies that also interfere. When national laws and technologies combine, concertedly, to interfere with the right to privacy in the name of national security, public safety, economic well-being, prevention of crime and disorder, the protection of health and morals, and the protection of rights and freedoms of others; then the landscape becomes, in a word, complex.

Remarkably, the ECHR has supported two privacy enhancing developments. First, the European Court on Human Rights has a rich history of reviewing states' laws and imposing sanctions on countries for failing to protect privacy adequately and proportionately. The interception of communications must be regulated carefully, according to jurisprudence. The court has also expanded the protections of Article 8 beyond government actions to those of private persons where it appears that the government should have acted to prohibit conduct.

Secondly, Europe is home to a remarkable host of privacy regulations in the form of data protection laws. The history is rich here as well. The first modern data protection law in the world was enacted in the Land of Hesse in Germany in 1970. This was followed by national laws in Sweden (1973), Germany (1977), and France (1978). These laws eventually led to the harmonising directive of 1995, the EU Data Protection Directive 95/46/EU.

This Directive provided consistent levels of protections for citizens and ensuring the free flow of personal data within the single market of European Union. The directive sets a baseline common level of privacy. In simple terms, it enforced the fair information practices that provides that

- *personal data should be collected only for specified, explicit and legitimate purposes*
- *the persons concerned should be informed about such purposes and the identity of the controller*
- *any person concerned should have a right of access to his/her data and the opportunity to change or delete data which is incorrect and*
- *if something goes wrong, appropriate remedies should be available to put things right, including compensation of damages through the competent national courts.* [2]

[2] European Commission. Data Protection in the European Union, available at http://europa.eu.int/comm/internal_market/en/dataprot/guide/guide_en.pdf

In essence, data should be collected with informed consent of the individual; processed fairly and lawfully, for limited purposes and limited use, and retained for a limited period of

time. Data must be kept secure and accurate, and not transferred to countries without adequate protection.

According to the Privacy and Human Rights 2002 report [4],

> *The basic principles established by the Directive are: the right to know where the data originated; the right to have inaccurate data rectified; a right of recourse in the event of unlawful processing; and the right to withhold permission to use data in some circumstances. For example, individuals have the right to opt-out free of charge from being sent direct marketing material.*

Meanwhile, tighter regulations apply to the category of 'sensitive data', defined as

> *data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs trade union membership, data concerning health or sexual preference. In principle, such data cannot be processed. Derogation is tolerated under very specific circumstances. These circumstances include the data subject's explicit consent to process sensitive data, the processing of data mandated by employment law, where it may be impossible for the data subject to consent (e.g. blood test to the victim of a road accident), processing of data has been publicly announced by the data subject or processing of data about members by trade unions, political parties or churches.* [5]

[3] European Commission. Data Protection in the European Union.

[4] EPIC. *Privacy and Human Rights 2002*: *An International Survey of Privacy Laws and Developments.* Washington, D.C.: Electronic Privacy Information Center and Privacy International, August 2002.

[5] European Commission. *Data Protection in the European Union.*

Member states may provide for additional exceptions for reasons of substantial public interest.

> *Such exceptions are permitted if, among other things, it is necessary on grounds of national security, defence, crime detection, enforcement of criminal law, or to protect data subjec*ts or the rights and freedom of others. [6]

These are consistent with the exemptions listed under the ECHR, while derogations also apply for data collected and processed for scientific or statistical purposes.

The European Union introduced the Telecommunications Privacy Directive in 1997. This directive applied specific protections to telephone, digital television, mobile networks and other telecommunications systems. Access to billing data was severely restricted, as was marketing activity. Information collected in the delivery of a communication was required to be purged once the call is completed. This Directive was planned for an update into the Electronic Services Privacy Directive in 2001 and 2002, which led to significant controversy, however.

In 2000, the United Kingdom proposed a policy to require the retention of communications traffic data for up to seven years by a central government authority. The proposal faced significant resistance in the public discourse at that time. But in December 2001 a similar policy was introduced and passed under the United Kingdom's anti-terrorism law in

Box 1-1. Fair Information Practices as in the EU Directive 1995. [3]

- Data must be processed fairly and lawfully.
- They must be collected for explicit and legitimate purposes and used accordingly.
- Data must be relevant and not excessive in relation to the purpose for which they are processed.
- Data must be accurate and where necessary, kept up to date.
- Data controllers are required to provide reasonable measures for data subjects to rectify, erase or block incorrect data about them.
- Data that identifies individuals must not be kept longer than necessary.
- The Directive states that each Member State must provide one or more supervisory authorities to monitor the application of the Directive. One responsibility of the supervisory authority is to maintain an updated public register so that the general public has access to the names of all data controllers and the type of processing they do.
- In principle, all data controllers must notify supervisory authorities when they process data. Member States may provide for simplification or exemption from notification for specific types of processing which do not entail particular risks. Exception and simplification can also be granted when, in conformity with national law, an independent officer in charge of data protection has been appointed by the controller.

response to the events of September 11, 2001. The new European Union directive on data protection in electronic services also supports the creation of such data retention laws within the European community and is consistent with international pressure to weaken data protection. In October 2001, President Bush sent a letter to the President of the European Commission requesting that the European Union "[c]onsider data protection issues in the context of law enforcement and counter-terrorism imperatives," and as a result to "[r]evise draft privacy directives that call for mandatory destruction to permit the retention of critical data for a reasonable period." Building on previously articulated concerns that "[d]ata protection procedures in the sharing of law enforcement information must be formulated in ways that do not undercut international cooperation," the United States Department of Justice submitted a number of recommendations to the European Commission working group on cybercrime [7], including the recommendation that

> *Any data protection regime should strike an appropriate balance between the protection of personal privacy, the legitimate needs of service providers to secure their networks and prevent fraud, and the promotion of public safety.*

This perspective was reiterated in May 2002, this time by the Group of Eight Justice and Interior Ministers [8], requesting that countries

> *Ensure data protection legislation, as implemented, takes into account public safety and other social values, in particular by allowing retention and preservation of data important for network security requirements or law enforcement investigations or prosecutions, and particularly with respect to the Internet and other emerging technologies.*

and included an official statement of how data protection regimes 'seriously hamper public safety'; and calling for the limited retention of data.

A number of policies have also been introduced to enable and promote increased data sharing, both within and across government agencies, and with the private sector. The sharing of data between agencies introduces purpose-creep where data collected for one purpose is used for another, but also introduces highly sensitive data to arms of government that can not be expected to protect the data adequately.

The United Kingdom is proposing "joined-up government" within its consultation paper on modernising government and public services to create "data-sharing gateways" and provide "seamless" services. It also tried unsuccessfully to allow practically any government agency to gain access to the traffic data of individuals under the Regulation of Investigatory Powers Act, including local councils and parishes. However, there are recent signs that this policy course is being reversed.

The increased flow of data is also coming from the private sector. The United Kingdom proposed laws to grant law enforcement agencies access to travellers' information. The United Kingdom Home Office has recommended that it gain access to information from every passenger before international flights; and it now appears that the U.S. requirements to receive passenger information from European airlines for the purpose of retention will go forward. [9]

Similarly, the European Union is considering granting Europol access to the Schengen Information System, including privileges to change the information held on travellers. Germany has recommended to the European Union the creation of a database of "known trouble-makers," to be used "for criminal prosecution purposes and in order to avert dangers constitute a proper and necessary tool in the fight against international terrorism. However, in view of the fact that members and supporters of terrorist groups are known to roam across Europe, the measure would be much more effective if it were applied by all European Union Member States."

Following from data sharing, there are a number of proposals to create profiles or increase the existing profiles of individuals. This occurs in a number of ways. The most immediate appears to be profiling travellers. In the longer term there are a number of proposals to increase profiling of citizens and non-citizens. These proposals are typically enhanced and complemented by national identification schemes, enhanced with biometrics. The United Kingdom is proposing the implementation of 'entitlement cards' in an effort to deal with immigration and illegal work, and identity theft.

None of the above trends are necessarily new; the novelty is the speed in which these policies gained acceptance, and in many cases, became law. In Section II of this report

[6] European Commission. *Data Protection in the European Union.*

[7] United States Government. *Comments of the United States Government on the European Commission Communication on Combating Computer Crime.* Brussels, December 2001.

[8] G8 Justice and Interior Ministers. *G8 Statement on Data Protection Regimes*. Mont-Tremblant: G8 Summit, May 13 and 14 2002.

[9] Council of the European Union. *New Transatlantic Agenda. EU-US meeting on Justice and Home Affairs*. Athens: EU, January 27 2003.

we will review some national policies and how they have been transformed under a number of imperatives.

Technology and Privacy Development in Europe

The Internal Market Directorate General of the European Commission argues that the concept of privacy enhancing technologies should best be understood in the context of the EU Data Protection Directive. Data security has for some time been an influencing factor in the design and development of Information and Communication Technologies (ICT). Many tools and projects (e.g. on encryption, digital signatures, biometrics, standards) are dedicated to its various aspects such as data integrity, authentication, reliability or access control.

However, the Internal Market DG also recognises that the key component to managing personal information was the minimisation of its collection and the purposes for which it is used. The relationship between policy and practice for the Commission was that "privacy enhancing technologies in this sense could be considered as providing a competitive advantage because they increase users' trust in the services and technologies involved." [10]

This drew attention to the various projects conducted and/or funded by the European Union. Since 1999 over 40 research projects have been supported by the EU under the auspices of the Information Society Technologies Programme Projects [11] that involve privacy and data protection management components to the research. The key projects are reviewed in section III of this report.

The actual adoption of PETs remains uncertain, however; as does their effectiveness. Recently, the Organisation for Economic Cooperation and Development conducted a study on privacy enhancing technologies [12], surveying member states.

> *Most respondents stated that technological solutions to protect privacy are implemented to a limited extent only, although some member countries (such as Japan, the United Kingdom, and the United States) indicated that the use of technical standards (such as P3P) to ensure compliance is expanding. The UK Information Commissioner promotes the use of privacy enhancing technologies, while in the United States there are many such tools widely available on the Internet (including P3P) but it is unclear how many businesses or consumers take advantage of them. The German Ministry of Economy and Technology has a programme to encourage the anonymous use of online technology. The Netherlands indicated that the Dutch government has committed itself to the use of privacy-enhancing-technologies in new public data processing systems. However, these initiatives remain exceptions. Otherwise, the use of technology to protect privacy was mentioned in the context of security. In Austria, as in other countries, the use of firewalls, anti-virus software and other safety precautions is standard, and the law requires certain data security measures but does not specify the exact techniques that are to be used. Finland indicated that the situation in companies varies to a great extent depending mainly on the size and partly on the field of the company.*

[10] Sottong-Micas, C., and Hillbrand, U. Privacy enhancing technologies: Looking for concrete answers. Brussels: European Commission Internal Market Directorate, December 1999. Available at http://europa.eu.int/comm/internal_market/en/smn/smn19/s19mn29.htm

[11] http://www.cordis.lu/ist/projects/projects.htm

[12] OECD. Report on Compliance With, and Enforcement Of, Privacy Protection Online. Paris: Organisation for Economic Co-operation and Development Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Technology, January 21 2003.

It is not surprising that the cause of security and privacy are often confused in the realm of privacy enhancing technologies.

In fact, it is questionable if many of the PETs that we casually consider as privacy enhancing truly perform this task in a verifiable manner, when placed side by side with the privacy regulations. While these technologies may provide confidentiality, it is not necessarily true that they therefore enhance privacy unilaterally. For example, encryption may be considered a PET, but when implemented into smart cards and a public-key infrastructure (PKI), it can support a national and virtual identification system more invasive than traditional paper-based cards.

As the EU moves towards e-government, in accordance with its own Action Plan for 2005 provision of services, the pan-European body acknowledges that there are challenges to the technological and legal differences among countries, particularly hinging on privacy. In the *Progress Report on the Development of e-Commerce and e-Government and the Role that Electronic Identification and Authentication Systems play in this Context*, released in December 2002 [13], the Commission noted that in the context of authentication and encryption and national identifiers,

> *Electronic identifiers are an expedient and reliable*

solution for the provision of e-Government services that make customisation of information possible to allow citizens and enterprises to fully interact with government online. They may, however, create specific risks for the privacy of citizens and the protection of their personal data and have to be assessed taking full account of relevant Community legislation, in particular Directive 95/46.

Further work is expected in this area from the EU, as the 'Working Party 29', the advisory body set up by the 1995 Directive, has decided to find ways to reconcile e-government with the data protection rules.

Alternative technologies are being developed in Europe. A significant number of PETs are being developed with government funding, through industry development, and even by individuals. A report from the Independent Centre for Privacy Protection Schleswig-Holstein [14] that focuses especially on privacy enhancing technologies that provide for transparency, data minimisation, system integration with built-in privacy protection, user-empowering 'do-it-yourself privacy protection', and multilateral security-systems, notes that in Germany alone there are over 13 PET development projects. Many of these are from individuals or academic

1-2. A listing of PET Development in Germany. [15]

GnuPG	Participation of Germans in the GnuPG ("Gnu Privacy Guard") encryption project. www.gnupg.org
GnuPP	"Gnu Privacy Project": GnuPG for everybody, launched in 2002. www.gnupp.de see http://www.gnupp.de/beteiligte.html#partner
Steganography	Development of steganographic algorithms and tools. E.g. http://wwwrn.inf.tu-dresden.de/~westfeld/f5.html. Technische Universität Dresden
BioTrusT	Research on and development of privacy-compliant biometrics with evaluation in some test scenarios, sponsored 1999-2002. http://www.biotrust.de see http://www.biotrust.de (among others: ULD)
"Anonymous Biometrics"	Development of some clever cryptographic mechanisms for protecting one's biometric data on the user's chipcard. http://www.iks-jena.de/mitarb/lutz/security/biometrie/security/ Lutz Donnerhacke, Jena
AN.ON	"Anonymity online – Strong Anonymity and Unobservability in the Internet", development and operating of an open source user software and a mix infrastructure, sponsored 2001-2003. http://www.anon-online.de (prior project: WAU – Webzugriff anonym undunbeobachtbar (Web access anonymous and unobservable)) Technische Universität Dresden, Freie Universität Berlin, ULD
rewebber	Anonymity proxy. http://www.rewebber.org Originally developed bei Fernuniversität Hagen.
DRIM	"Dresden Identity Management" (part of PRISMA), will be presented at CeBIT 2003. Technische Universität Dresden
PRIMA	Prototype for an identity management proxy, presented at CeBIT 2002. Universität Darmstadt, T-Systems.
PRISMA	"Privacy-Rich Identity and Security Management", design of a reference architecture of privacy-enhancing identity management integrating convertible credentials with research on legal, sociological and usability aspects. The consortium has been working together since 2001. PRISMA will be a subproject in the PIMIP proposal (Privacy and Identity Management Integrated Project) for the 6th Framework Programme for Research and Technological Development of EU. ULD, Technische Universität Dresden, IBM Research Lab Zurich, Karlstad University .
Study	IMS EU Study "Identification and Comparison of Identity Management Systems", applicant: Joint Research Centre Seville. ULD, Studio Notarile Genghini (Milano)
Privacy	Model Privacy-Enhancing Design of Security Mechanisms, http://www.cs.kau.se/~simone/, http://link.springer.de/link/service/series/0558/tocs/t1958.htm Simone Fischer-Hübner, Universität Hamburg.
DASIT	"Datenschutz in Telediensten" / "Data Protection in Tele Services", Privacy Protection in the Internet by User Control, since 1998 development of a prototype for helping users asserting their privacy rights online. http://www.sit.fhg.de/german/MINT/mint_projects/project_pdfs/dasit.pdf see http://epso.jrc.es/newsletter/vol09/4.html

researchers.

[13] Council of the European Union. *Commission Staff Working Paper – Progress Report on the Development of e-Commerce and e-Government and the Role that Electronic Identification and Authentication Systems play in this Context*. Brussels: European Commission, December 4 2002.

[14] Hansen, M. *PET in Germany*. Kiel: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, November 2002.

[15] Hansen, M. Pet in Germany.

All this development only represents Germany. We review the developments within France, Finland, Denmark, and the United Kingdom in section II; and again this is only a small component of the work being conducted.The largest research and development initiatives are either private or EU-funded research projects, as mentioned above, and these will be investigated in Section III.

The following report presents a snapshot of the privacy and technology issues in Europe. Europe is a continent with countries with their own rich histories, cultures, and legal contexts. We are now considering the context of technologies, new systems of governance, and new regulations within this 'Information Society'. The challenges for the existing structures are clear enough: deliberative democracy is a complex system even without the additional factors of data flows, information technologies, and trans-jurisdictional policies. Europe is unique in this sense, but perhaps also a benchmarking case as our world becomes increasingly linked and heads towards heterogeneity and homogeneity.

Section II. Country Reports

Introduction

Nations are like people: each must deal with change in its own individual way. The advent of the Internet has posed the same questions to every country, but each answers differently depending on its cultural, economic, and legal background. The effort to move towards e-government on the parts of four countries — Denmark, Finland, France, and the UK are discussed here. All are European, and therefore to some extent functioning within the same legal structure. Yet each has responded very differently to the same set of problems, which are common to all developed nations. Increasing bureaucratic complexity makes it frustrating for their citizens to gain access to the benefits and services they're entitled to. Governments want to cut costs and improve access to services by taking advantage of the Internet and related technologies. Every country struggles with trying to protect its culture and traditional freedoms while moving into the electronic age in which so much more is visible.

All these countries have in general relied on legislation to protect individual privacy, rather than promoting technology. This is for a variety of reasons. France has regarded strong cryptography as something only the government should use, and by regulating it has limited its adoption to enhance privacy outside of a few specific areas. One of these exceptions is smart cards (particularly banking and credit cards), of which France is probably the largest user (and developer-manufacturer) in the world. In Denmark, trust in government is so pervasive that PETs have not been thought necessary. Finland is home to a number of companies producing related technology. In the UK, two factors have contributed to the general non-use of PETs. First, most people do not understand or are not aware of the technologies involved. Second, the government has consulted the public very little when formulating the invasive laws of recent years that regulated their use; as a result the public is not really aware of the potential of these technologies.

In most cases in all four countries, therefore, privacy is protected by law, not technology. Only the two Scandinavian countries have the right to privacy explicitly written into their constitutions. France's courts have ruled that the right to privacy is implicit in its constitution. The UK, of course, has no written constitution, and a legal basis for privacy only began in 1984 with the passage of the first Data Protection Act. Even this law was resisted by the UK for some time. It may not be coincidental that the UK has the most invasive laws, most of them passed in the last few years. A number of these proposals have mirrored similar proposals in the US, which the UK tends to feel is closer in culture and legal system than the rest of Europe. However, clauses in the American constitution constrain successive American government administration from introducing, as formal policy, some of the worst proposals that have passed in the UK.

In the other countries, increasing surveillance and monitoring has more to do with what American essayist and software engineer Ellen Ullman called "the fever of the system" in her 1997 book Close to the Machine. Based on her personal experience designing a database for an AIDS project, Ullman notes that given a new database humans often lose sight of their original benevolent objectives. Instead, she says, the computer infects them with the desire for increased surveillance simply because the option is now available. People with two databases inevitably want to link them together. People desigining a system to help AIDS patients get all the benefits they're entitled to suddenly ask if that system could also check that no one's getting anything extra. And so on.

Ullman's "fever of the system" can clearly be seen at work in these countries as they consider new possibilities. France, for example, like Finland, has a complex web of intersecting laws. However, France's most important safeguard is a unique commitment to what it calls the "non-crossing" principle. Simply, the non-crossing principle is a prohibition on sharing data between databases and departments. This principle has been applied over and over again in the history of French administration, and remains a vital stumbling block as France tries to move its administration into the electronic era. For probably the first time since its adoption in the 1970s, French politicians are beginning to argue that the principle may no longer be relevant. Because: it's an impediment to e-government.

The UK has been infected the same way. Tony Blair's Labour government reiterates frequently the importance of offering citizens "joined-up government". "Joined-up" is a phrase that may being confusing to those outside the UK. It is a term taken from handwriting. Printing, which is learned first in school, is made up of all separately drawn letters. Joined-up handwriting, which you learn later, flows smoothly from letter to letter. So Blair's term implies both a sense of data flowing smoothly between departments – which is supposed to make life easier for citizens – and a sense that this style of government is somehow more grown-up than the compartmentalised system the UK has now. The further implication, of course, is that it's somewhat childish to object to the joining-up.

Denmark is the only country in this group that adopted cross-linking via a single national ID number as early as

1968. National ID numbers, which will inevitably make up part of the UK's proposed "entitlement card" scheme, are used for everything in Denmark, from taxes to travel cards. The result is a society of extreme transparency, even though privacy is a core value in that country. A reason why this works is the highly unusual level of trust by Danish citizens in their government coupled with a value for efficiency. It may help that Denmark's traditional prosperity has allowed it to offer a complete system of benefits to citizens. Nonetheless, Danish observers say that under the pressure to bring in electronic services, the social contract that has nurtured this trust is beginning to break.

The section that reports on Denmark's experience is particularly important reading for anyone considering creating a national ID system or creating a fully transparent society. What has apparently succeeded in Denmark is unlikely to work anywhere else. Worse, if the social contract that has made Danish transparency possible now breaks, Denmark will have to completely reinvent its systems to include PETs and less transparent multiple IDs.

Every country must also meet the expectations of its populace. This is particularly true in the area of privacy, where feelings can run very hot. Even the UK population, which in general has objected very little to the widespread deployment of such privacy-invading technologies such as closed-circuit TV cameras, can be roused to anger if it believes the government has gone too far. An example of this happened as recently as the summer of 2002, when the current (Labour) government proposed a list of more than 200 agencies it thought should have access to retained communications data. The public outcry forced the government to withdraw the list and reconsider. A similar level of protest is brewing over the proposals for an "entitlement card" — a national ID card by any other name.

National ID cards, are however, a perfect example of how different cultures among countries can be, even within Europe. Opposition to national ID cards is a visceral, deep-rooted component of British culture. Proposing one reminds people of World War II, when national ID cards were deployed as part of wartime national security. Because of this widespread antipathy to ID cards themselves, the current government has been careful to include in the proposals for an "entitlement card" the proviso that it would not be compulsory to carry the cards. In other words, the government is proposing a giant national database rather than specifically a card. Yet Danes have had such a thing for more than 30 years with none of this cultural baggage attached to it.

Since all four of these countries are members of the EU, the four share a common need to support EU privacy, data protection, and human rights. Each country, therefore, has had to pass national legislation to meet a common set of standards. Yet the impact is very different in each country. France has taken so long to pass amend its existing data protection legislation to support the 1998 EU Privacy Directive that the EU has brought legal action against it. Denmark, on the other hand, has actually had to water down its laws because they were actually tougher than the EU requirements. In Denmark's case, harmonisation may actually have cost the country some of its traditional privacy protection.

Also highly noticeable is the different level of familiarity with and usage of privacy-enhancing technologies. Of the four countries examined here, only Denmark has failed to consider such technologies at all. Probably, this is partly because of that culturally odd high level of public trust in government. Also likely to be a factor, however, is that Denmark is not in general a haven for high-tech innovation, and it is the only country in this group without significant PET products and/or research. Finland is home to the mobile phone giant Nokia and many other high-tech companies, as well as being the native country of well-known names such as Linus Torvalds, author of the open-source software Linux. Even so, only France has used PETs in a systematic way by deploying smart version of credit cards to prevent fraud; the cards themselves are not PETs, but encryption is deployed on the cards, which can be interpreted as being a PET.

This is particularly ironic, as France has the strictest regulatory regime for strong cryptography – probably the single most important PET. There are two consequences of this. First, a higher level of cryptography activism is to be found in France than is presently to be found in most other countries, apart from the noteable case of Germany. Second, there is little in the way of products marketed in this sector. Other countries have had significant battles over cryptography. But in the UK, for example, these battles ended in 2000 with the passage of the Regulation of Investigatory Powers Act. After much opposition from organisations such as the Foundation for Information Policy Research, requirements for storage of decryption keys with third parties were dropped. Since then, while research in this area has continued, particularly at Cambridge University, other subjects have become more important for privacy activists to pursue.

What seems to be characteristic of anyone infected with the "fever of the system" is a high level of what Orwell called "double-think" — that is, the ability to say one thing and do another without noticing the disparity. Everyone claims to want to protect traditional freedoms. Everyone claims to value privacy, freedom of speech, and the right of citizens to access public information and control public access to their

own personal information. Yet in Denmark PETs have not even been considered for deployment in new e-government services, and in the UK there has been no public discussion of for example whether to accept payment via anonymous cash for smart card travel tickets or London's congestion charge. Meanwhile, at least some French politicians seem to be in the process of convincing themselves that their society could be freer if only France were more transparent — like Denmark.

It is important to remember when designing "Information Age" systems, that CCTV, travel tickets, and even digital rights management are only the beginning of the invasive technologies we can create and deploy. The UK already boasts it has one million samples in its DNA database, and France has set matching that figure as a goal. It is not just the privacy of our homes, movements, and thoughts that is at stake. It is the privacy of our very selves.

Like security and environmental protection, privacy is not something that can be easily added to a system after it has been designed. If a system generates data, sooner or later someone will decide to retain it, mine it, and access it. This principle can be seen at work in the way UK boroughs have retained CCTV footage, or in the decision by the transport company in the Finnish capital of Helsinki to retain travel data for later retrieval. Therefore, the time to consider whether and how to deploy privacy-enhancing technology is when the system is being designed. Privacy must be a consideration from the beginning, and must be built in from the ground up. Culture and law should dictate the design of technology to protect the rights of individuals. Technology should not dictate culture and law.

Privacy Enhancing Technologies in Denmark [16]

I. Introduction

Historically, Denmark has been characterised by public efficiency, public trust in government, and economic prosperity including a welfare system to take care of the weak in society. During Denmark's attempts to make the transition to the "information society", it is trying to find ways to protect all four of these values — privacy, trust, efficiency, and prosperity — at the same time.

Danes' trust in their government is based on a form of cultural social contract between citizens and state, combined with a tendency to choose pragmatic co-operative solutions early. Examples include the still-unique Dankort (joint credit card clearing), the efficient Value Paper Clearing House, and the CPR system.

Danes enjoy considerable legal privacy protection. However, Denmark adopted a system of national ID numbers for its citizens as long ago as 1968. By now, the Central Person Register (CPR) number, as it's known, is used as an identifier in almost every aspect of Danish life.

Danish philosopher Ole Fogh Kirkeby [17] recently suggested that within public administration the traditional culture of the civil service is eroding due to the introduction of business management culture. Emulating the private sector leads to a narrower focus and less loyalty to the whole. Denmark's relatively high level of efficiency and trust in government is the starting point for this discussion. It has persisted so far, even though from a power perspective citizens are in relatively little control. Very detailed data are stored in databases easily linkable though Denmark's numbered national ID system. The only protections are legal and cost boundaries.

Denmark is unique in two ways. First, because so much is integrated around CPR numbers. Second, because Danes express one of the globally highest levels of trust towards their government [18] – even higher than other Scandinavian countries. It should be strongly underlined, however, that it is a mistake to use Denmark as an example to make the claim that national IDs are or could be positively correlated with trust.

Special cultural aspects are involved here. Denmark seems to be governed by a sort of cultural social contract, as Dutch cultural scholar Geert Hofstede has pointed out. Scandinavian, and especially Danish, culture is unique in terms of having both a low power index and a low uncertainty index while retaining a high sense of group cohesion (feminine values). Neither abuse of power nor its accumulation is accepted or expected.

Trust in the private sector is low, but the public sector is historically seen as a friend preventing abuse. Even so, this trust has not turned naive [19]. Preventing abuse has historically been a core element in the strong Danish civil servant culture, which can be characterised by strength of purpose and commitment to serving the citizen. The results can be seen, for example, in Denmark's generally low level of corruption and its stability across changes in government.

[16] Stephan J. Engberg is member of the International Advisory Board of Privacy International and founder of Open Business Innovation (www.obivision.com), member of EUs Network of Excellence in Privacy & Identity Management, working commercially with Privacy Enhancing Technologies. He is lecturing in Privacy Marketing at various post-graduate courses at Copenhagen Business School and IT University.

[17] Loyalty, Ole Fogh Kirkeby, 2002 (http://cbs.dk/staff/ole.fogh.kirkeby/publ.htm)

[18] World Economic Forum 2002 Trust Survey (http://www.weforum.org)

[19] A large survey from 1999 pointed towards a clear reluctance to show VERY high Trust (http://www.sociology.ku.dk/vaerdi/ddvhome.html)

Statement from the Danish Ministry of Science, Technology and Innovation:

Political aims in Denmark — Privacy

eGovernment in Denmark

The goal of the Danish government IT- and telecom policy is clear. It aims to contribute to:

- Create growth in Danish private sector.
- Reform the public sector.
- Qualify Danes for the future information society.

The Danish government want seriously to receive benefits from IT-investments in the public sector. It is among the government political aims that:

- The public sector works and communicates digitally internally and externally with citizens and companies.
- Public services are centred around citizens, making increased reuse of public data and a growing number of horizontal public portals.
- Focus is increased and organisation strengthened related to the IT-area.

Privacy Principles

The Danish Government focus on a better use of IT opportunities in the Public sector rests on three basic assumptions:

- IT shall contribute to effectiveness in the public sector
- IT shall contribute to make the individual citizen experience a better and more flexible public sector
- eGovernment may not lead to reduction of citizen rights.

The Policy to promote citizen use of intern towards the public sector and simultaneously ensure citizen privacy is based on among others the following laws:

Freedom of speech

- Constitution
- European Human Rights
- Criminal law

Registration and surveillance

Personal Data Protection Act (Persondataloven)
Data Protection Agency guidelines No 126 dated July 10, 2000 on Registrant Rights
Law on Digital Signatures
Law on certain consumer agreements (Dørsalgsloven)

Information about privacy concerning use of the internet:

IT-Security Comity publication on Privacy on the Internet
Status report on citizen IT-rights
Legal information homepage (www.retsinfo.dk)

Present projects in Denmark

In addition to the above status the present actual projects have relevance to the question of Privacy Enhancing Technologies in Denmark:

- ESDH-project (standardised business file management)
- Digital signature
- Webreg (company registration)
- E-boks (centralised storage of public and private electronic mailings)
- EPJ-project (electronic healthcare)
- E-dag (change to electronic communication intra-public sector)

II. Legal landscape

Privacy is written into the Danish Constitution of 1953. Section 71 holds personal liberty to be inviolable. Section 72 considers home, communications, and personal files inviolable. Exceptions are allowed only if the violations are subject to a judicial order. In 1978, the Danish Parliament passed the Private Registers Act to regulate public-sector activities in data protection. Finally, in 2000 the Act on Processing of Personal Data came into force as national legislation implementing the EU privacy directive. According to this last law, personal information may be classified as ordinary, semi-sensitive, or sensitive. Different processing conditions apply to each classification.

Data protection regulations are enforced by the Data Protection Agency (Datatilsynet), overseeing both public and private databases and registrations. Most interestingly, the 2000 Act requires that the DPA give an opinion before the issuance of any new laws or regulations that have an impact on privacy.

A number of other laws also protect privacy by setting out basic principles for the treatment of personal data, sometimes in a sectoral manner. There are also laws to regulate access to information by the public. These laws actually take precedence over the generalised Data Protection Act, provided that they are in accordance with Denmark's international and community obligations.

Denmark also has other general laws that act to ensure citizen access to personal data and to require citizens to give permission for such data to be held in both public and private databases. Special regulations cover the management and use of personal data without permission by public administration and infrastructure. There are no technological control mechanisms implemented beyond logs and traditional security to block unauthorised access.

There are alarming legal developments, however. According to a June 2001 policy, police may access a list of all mobile phones that were in operation near the scene of a crime at the time the crime was committed. In June 2002, Parliament enacted a law establishing mandatory retention of communications traffic data for one year and allowing law enforcement to install monitoring software on computers to record keystrokes. Finally, immigration authorities may require DNA samples from applicants for residency.

All of this is in addition to the ubiquitous use of CPR numbers in Danish public and private life. Denmark is highly integrated around a single national ID number known as the Central Person Register number (CPR number). The CPR number, which consists of a person's birth date plus four digits, was introduced in 1968. It is used in all aspects of public administration and most areas of commercial activities that involve reporting to public authorities for tax, employment, healthcare or other public services.

More than 30 years of gradual introduction of CPR numbers mean that despite initial premises to restrict the use of these national ID numbers, function creep has been close to all-encompassing. As such, vertical integration from individual citizen through intra-unit processes to national statistics is almost complete. Horizontal data-sharing across units has been restricted by legal mechanisms, but the technical barriers are low.

The extent of this practice is best illustrated by the fact that a tax return in Denmark is completed by simply signing a pre-prepared statement from the tax authority, ToldSkat, or Central Customs and Tax Administration. Even access to public libraries is linked to CPR numbers. Danmarks Statistik, the national Danish statistics office, claims to have the most comprehensive database of citizens in the world, covering 30-plus years of details from all areas of life, linked together with individual ID numbers.

Overall, Danish privacy rests on its complex system of legal permissions. There have been few or no attempts to introduce PETs.

But although the above solutions have traditionally provided privacy in the physical world, they do not provide the same protections when translated into the digital world. Without PETs, there is no digital equivalent of physical, anonymous cash, and all transactions are recorded and linked to individual citizens. Yet Denmark persists with a unilateral approach to security (from a privacy point of view) that relies on identification and transparency. The system assumes complete trust and affords only legal methods of privacy protection.

III. Transformations in policy and technology

Because of the high level of trust in government, traditionally the focus of Denmark's privacy laws has been on protecting citizens from private sector abuse. Technological examples include the credit card clearinghouse (PBS), which is a central banking service clearing all payment transactions in a highly linkable manner. This is NOT a strong privacy solution, but even so merchants are not allowed to access credit card numbers for the purpose of linking transactions. Similarly, banks are not allowed to datamine payment transactions for purposes such as credit scoring.

Payment data are linked and available to make it possible to trace fraud. Such data could – but may not – be used for other purposes. Denmark has no shared database of credit

ratings, although it does have a shared "Bad Credit" (RKI) file. Strong legal controls regulate the use of and updates to this blacklist.

The government has said of its own strategy, "High security is a vital precondition for e-government. The public needs to have full trust in the systems to use them, and the public sector needs a high level of security to handle a large part of the electronic contacts with citizens. A digital signature for citizens, companies, and public institutions is a major component of this strategy." [20]

[20] e-government strategy document

Despite clear statements from citizens that increasingly surveillance and registration are taking control, the focus on identification remains unilateral. If citizens demand control – as documented in the Healthcare report discussed below – this approach to trust is a high-risk policy. Without trust, this intellectual approach to privacy may collapse, leading to a rapid change in public attitudes. Continued progress towards a transparent and always identified society may erode the critical trust towards government. It is a dangerous road, or even a blind alley, to pursue.

Like many countries, Denmark is increasingly focusing on finding ways to combat benefit fraud, fight against terrorism. The new rules allowing data retention and data-sharing could mean that Denmark is in a phase of transition. The increasingly visible transfer of data control from citizens to public IT systems may change the nature of trust in government. Increasingly, trust may be based on fear or distrust (have to trust) rather than being a result of non-invasive government behaviour (no reason not to trust). At the same time, although public trust in the private sector has always been low, the dot-com crash has made things worse. The corporate sector in Denmark was hit just as hard as the rest of the world, creating a crisis in on-line trust. Danish authorities, like others everywhere, are failing to resolve this crisis.

Significant effort has been put into speeding the transition to e-government in order to harness the potential for efficiency. The result will be to turn Denmark into a very transparent country based on direct or indirect identification directly related to CPR numbers. Denmark is far along in this transition, which is only partially recognised internationally. Overall, Danish public administration is already highly vertically integrated and is now moving towards horizontal integration and cross-boundary process support that increasingly relies on reusing citzen data. The traditional values of trust, legal protection, and efficiency may not extend into e-government.

But indications are emerging that the social contract for trust is starting to break. The erosion of trust potentially risks damaging both efficiency and the perception of privacy. The trust problem is increased by the general invasion of technology into personal lives. Citizens report a sense of loss of control and distrust due to growing monitoring and registration.

These trends have of course been documented. A report from a 2000 Danish technical conference on electronic surveillance [21] discussed many potential consequences of the noticeable growth in surveillance and registration. These included personal alienation and the threat to the individual as the core of democracy. Even though the report mentioned some options such as proxies, awareness of asymmetric identity and privacy-enhancing technologies is very low. This is backed up by focus group surveys reported in a 2003 Technology Outlook report on Pervasive Computing [22] from an expert group organised by the Danish Ministry on Science, Telecommunications and Technology.

Unfortunately, the consequence is that everyone assumes that problems are almost unavoidable. A few experts have gone so far as to claim that the fully transparent society was actually freer. Overall, using technology to reduce the negative trade-offs of increased surveillance and registration is not even considered. In short: the problems and risks are known but in reality are ignored except in words.

The digital world is a world of growing risk of abuse of personal data. More people can access more data in more databases and there are more tools to collect, analyse, share, and retrieve these data with increasing computational power at decreasing cost. Trust — through its correlation with risk — is increasingly under pressure from all sides in the digital world.

These changes are very recent. Citizens are only starting to be exposed to the effects of the reduced legal protection afforded by the looser data protection laws introduced in 2000 to harmonise with the lower level of protection given by EU level. The combination of relaxing laws and new digital threats to privacy provide a dangerous trust platform for e-government.

This view was expressed in a 2001 report from the Danish Technology Council on local e-government where a citizen statement was included to the effect that, "I have to trust them – otherwise I would have to be suspicious all the time." [23] The report otherwise noted positive attitudes towards the idea of e-government.

The gradual shift from trust in public authorities towards a desire to retain control of personal data was expressed and emphasized in a 2002 Citizen report [24] on HealthCare files from the Danish Technology Council advising the Danish Parliament. This statement was the result of a

representative group of citizens selected to provide an informed opinion based on consultation with experts and public officials on HealthCare issues.

Even though firm conclusions are not possible yet, indications are that the traditional platform for trust in the Danish society is being challenged by the transition to the digital information society. Since these effects are already measurable it would be a mistake to assume that the traditional level of trust will survive.

[21] Electronic Surveillance, Teknologirådet 20009 (http://www.tekno.dk)

[22] Technology Outlook/Teknologisk Fremsyn 2003 (http://www.teknologisk-fremsyn.dk)

[23] Local eGovernment (http://www.tekno.dk)

[24] Danish Technology Council / Teknologirådet - Panel on Patient Files (http://www.tekno.dk)

IV. PETs and Denmark

Perhaps the biggest danger of all to public trust is not trying to do better. The problem is not so much naiveté so much as it is a lack of understanding of the potential of privacy enhancing technologies.

Around the world, the use of PETs has been strongly correlated with the presence of data commissioners who take an active view and accumulate knowledge about the use of technology to protect privacy. This has not been the case in Denmark, where protection of privacy has traditionally been achieved with a combination of legal and control mechanisms combined with pragmatic technology solutions.

In autumn 2002, the Danish Consumer Council announced a change in policy by calling for technical solutions to protect consumer privacy from digital privacy threats. However, no privacy-enhancing solutions have yet been introduced.

Three case studies follow to illustrate various aspects of privacy in e-government. Healthcare is the most complex and by far the most sensitive. It is also the most quality-focused and cost-focused of the three. The remaining two look at controlling benefit fraud and cross-sector analysis and data access. The latter are mostly used for research.

In all three cases, PETs could help protect privacy, but there are no known efforts to find or deploy appropriate technologies.

Health Care

The privacy aspects of security are more obvious in health care than in any other sector. Data are important for efficiency and quality, but confidentiality is absolutely essential.

Digital support of Danish health care is on a fast track, with ambitious plans to cover all hospital beds with cross-country semantically integrated electronic patient files by 2005. "Semantic" means optimised for automation and data reuse without requiring human intervention. Multiple processes are being developed to support cross-sector data sharing such as for instance between general practitioners, hospitals and distributed care services.

On the surface, it looks as though the system maintains strong privacy and confidentiality. Except in emergency situations, where the patient may be unable to consent, there are strict requirements that patients must give permission before their data can be shared. However, a closer look at the security guidelines [25] reveals a different story, as these emphasise access and efficiency over privacy.

Patient files will be comprehensive, covering still more areas related to healthcare. These records will be stored in multiple central databases indexed by CPR number, and secured only by traditional access controls. The envisioned security system assumes the infrastructure will be a large secured intranet, even though there will be thousands of access points available and the government expects increasingly to outsource public services to the private sector.

There are no plans to require or implement identity protection schemes such as pseudonyms or real linking of permissions to access control. On the contrary, the security guidelines for access control systems are explicit in stating [26]:

> *"Access control to patient files therefore cannot mean that the system merely refuse the caretaker access to the desired information, but should instead provide several levels so that the caretaker can change to a level with extended access. When changing to this level a warning to the caretaker of imminent unusual behaviour incl. a special marking in the logfile should be given for instance through a special window. It must be possible to pass this window with a simple key press indicating the unusual behaviour is valid."* [27]

[25] Healthcare Security (http://www.sst.dk/faglige_omr/informatik/sikk/infosikker.asp)

[26] When making access control systems in Healthcare it should be noted that not having access to data can cause death of the patient and the patient in critical situations often is unable to provide access himself. Privacy access control therefore needs advanced solutions.

[27] Health Security Guidelines, p.37.

Citizens request privacy control of exactly who can access their data, but this desire will probably be ignored in the technical design and only honoured within the above privacy paradigm based on general level clearance and log files. Legally, patient permissions are required to access healthcare data, but

these permissions are treated in the context of legal compliance only - not implementing real limitations on access control. Sensitive health data will be easily available to a large group of IT systems, care personnel and system administrators without even considering implementing PET solutions.

Control of benefit fraud

Local and social sector authorities are focusing strongly on detecting and stopping social fraud. Few legal restrictions are in place to protect the privacy of citizens.

The desire to detect social fraud is driving the compilation of dossiers on individual citizens for any number of the many subsidy programmes within the Danish welfare system. There have been recent legal debates and restrictions over whether local authorities are allowed to put citizens under surveillance in the interests of detecting fraud such as fake marital separations, private use of company cars, or unregistered working on the part of the unemployed. [28]

Research, process control or quality assurance

The growing pressure to provide efficient and high-quality service as well as the demands of medical research and process quality is also driving the development of very detailed dossiers. Increasingly, these are enriched with specific information about individual citizens . [29]

Large central databases are being created that cover all medical prescriptions and purchases, linked to both CPR numbers and the doctor who wrote the prescription. The goal is to limit growing medical expenses. Also under implementation are large centralised databases intended to help track the quality of individual treatment across units.

Anonymisation is not possible for research linking multiple sources or time periods.

[28] Danish Parliament Online and media coverage

[29] For instance the National Indicator Project (htto://www.nip.dk)

V. Other issues

Several other notable changes in Danish culture are worth discussing in this context.

Increasing links between public and private sectors

A new trend is the redistribution of personal data that has been collected and stored for commercial purposes such as housing files (BBR) and on-line access to previously paper-based collections of data such as collaterals. Also new is the ability to micro-segment data (Danish Statistics such as Mosaic), "wash" customer databases against the main CPR files, share "bad credit" files, and so on.

An important issue to consider is whether the separation between public and private sectors remains relevant in the digital age from a trust and privacy perspective. Instead the focus should now be on who is in control of the data – the individual or the system.

Portals: concentrating security risks

Present planning is to introduce portals in the interests of convenience and efficiency. But portals based on CPR numbers also establish a single point of security failure. Both break-ins or internal security breaches can expose or provide horizontal access to large amounts of citizen or corporate data.

Chipcards/Digital Signatures

The largest Danish Telco, TDC, recently was awarded a contract to introduce free soft key digital signatures to the full population in collaboration with the IRS [30]. Technical specifications for anonymous certificates are included, but are not promoted and the procedure for the trusted party to release identity does not require a court order.

Negotiations are carried out on how to progress this softkey solution to a smartcard solution. In this case, technical methods for protecting privacy and privacy issues generally have been included in the process. [31]

[30] Ministry of Science, Technology and innovation (http://www.vtu.dk)

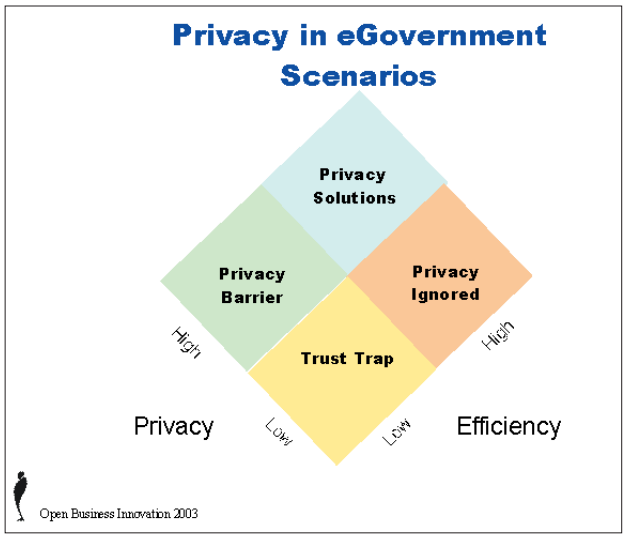
[31] Report on Business opportunities in multi-application Chip cards (http://www.oem.dk)

VI. Implications and conclusions

Two key measures are relevant when trying to consider the future development for privacy in a system of Danish e-government. First is the level of efficiency measured relative to international levels. What was efficient yesterday may be average today and below average tomorrow. Second is the balance of power between citizens and state measured as privacy or power distribution of personal data. This discussion considers four scenarios that can be diagrammed in a two-by-two matrix as shown in Figure 1.

Present trends are clearly moving towards the right – that is, towards sacrificing privacy in the interests of efficiency. Few if any efforts are in the pipeline to provide further protection of privacy. Numerous efforts are ongoing to add types of data that have not previously been included to those already available in digital format. In addition, the drive is underway to increase data sharing across sectors and compile detailed profiles from a number of perspectives for specific analysis. In addition, the general commercial and technical trend toward a transparent society will provide serious threats to privacy.

From here, four different scenarios for the future are envisioned.



Privacy Ignored (Passive Acceptance)

In the Privacy Ignored scenario, government favours efficiency over privacy. Citizens feel the problems of loosening control and perhaps increasing alienation but give up trying to change the trend towards a transparent society in which all transactions are identified.. Lightweight PETs such as P3P might slow the development of this scenario, but each move toward less privacy will help arm a potential trust bomb composed of growing risk of abuse. Given the present growth in privacy awareness and given that citizens are starting to notice a shift from trust towards a desire for control, this scenario does not seem sustainable.

Trust Trap (Passive Resistance)

If the traditional trust model does not prevail, Denmark could end up in a Trust Trap characterised as a low-trust scenario with both low privacy and low efficiency. Invasive e-government solutions combined with generally hostile technological development pushes Denmark enter into a phase of trust destruction and passive resistance eroding the traditional strength of Danish society. Citizens object to the Information Society and passively act against it, blocking the realisation of its full potential. This scenario is very similar to the trust crises already emerging elsewhere in the world and therefore seems a likely possibility.

Privacy Barrier (Active Resistance)

If the trust bombs blow or Danish citizens otherwise feel their trust towards government has been betrayed, Denmark could face growing privacy barriers. In this low-trust scenario, increasing privacy activism means that citizens actively resist developments. Resistance halts, delays, or seriously changes e-government programmes and forces tight control of public sector use of consumer data. This scenario could develop as the consequence of a major security failure in for instance the tax, health care, or welfare sectors. A political consensus banning the transfer of more control from citizens to government would block the desires economic efficiencies and service quality.

Privacy Solution (Active Acceptance)

The sustainable high-trust scenario is the scenario in which an active decision to introduce PETs to eliminate or reduce trade-offs between efficiency and privacy. In Denmark a move to dismantle the national ID system is not likely. Instead this scenario would incorporate a gradual transformation of the existing national ID structure into one using multiple IDs.

The main differences between a proactive decision on the part of government and a change forced by citizens will be trust and cost. When citizens start demanding the incorporation of PETs into public systems, it will be both because trust has already been eroded and because the investment made in the digital transition have been used for non-privacy solutions.

Conclusions

Historically Denmark is characterised by high public efficiency, high citizen trust towards government and economic prosperity including a welfare system taking care of the weak in society. Maintaining this remarkable attractive position require that the difficult transition phase to the Information

Society is successful simultaneously improving both the quality and efficiency and citizens trust towards Government.

NO attempt should be made to copy the Danish model internationally. Only special Danish cultural conditions made it possible, and the new digital challenges are making the sustainability of this approach questionable. The totally transparent society linked to a single national ID increasingly looks like a blind alley.

Even if the current citizen/government trust model holds, it is unlikely to be extensible to the private sector without new security mechanisms including some kind of PETs. Consumer trust towards e-commerce is too low, and the privacy threats too obvious.

The Danish challenge lies in learning to question the intellectual and cultural assumptions that led to the CPR number system. The best Danish option is liekly to use the transition phase to redesign the national ID system using PETs and move to a more advanced multi-identity national ID system in order to return control to the citizen. Such a move would simultaneously achieve security and efficiency while ensuring citizen trust and privacy.

Privacy Enhancing Technologies in Finland [33]

I. Introduction

Finland is infamous in privacy circles for its national identification numbering system. As it started in the 1970s, the number is use extensively in both public and private sectors, on passports, driving licenses, and various data files. In 1999, however, the government began issuing new cards using smartcard technology, including certified digital certificates. There are also plans to put them in the SIM cards in mobile phones and interactive television systems.

Once all this information is within government databases, the concern that naturally arises is that of security. Most Finnish public administration is covered by some kind of information security policy. In the most advanced units, the information security administration system covers the main elements in information security, from planning to implementation and monitoring. Some organisations have already gained a BS7799 information security certificate. [34]

Electronic transactions, information security and data protection in health care have been developed in a variety of pilot projects. Electronic patient cards, secure identification of users and electronic communications encryption have all been introduced for public sector use.

Within central government, information security matters are distributed among a number of parties. Within local government, the situation varies. On the whole, however, exactly who bears responsibility for developing information security is not sufficiently clear. If a local authority's IT systems are linked to central government IT systems, the Ministry of the Interior is in a position to exercise guidance. The Advisory Committee for Data Management in Public Administration (JUHTA) and the Association of Finnish Local and Regional Authorities also provide information security guidance, but otherwise local authorities operate independently. [35]

[33] Herko Hietanen and Mikko Valimaki.

[34] http://www.c-cure.org/

[35] FICORA Report: Information Security Review Related to the National Information Security Strategy
http://www.ficora.fi/englanti/document/review.pdf (FICORA Report)

Legislation and rules regarding information security solutions are being developed both nationally and in international cooperation. There are several current topics: responsibilities in e-commerce, issues in identification and digital signatures, creation of a public key infrastructure and its regulation, and information security requirements to be made of service providers and operators.

It should be noted that Finland has an extremely open policy about state and municipal documents. The right of access is enshrined in law, enforcing the duties of the authorities to promote openness and good practice on information management in government, and to provide private individuals and corporations with an opportunity to monitor the exercise of public authority.

Large companies are generally active in information security, although their level of competence varies. Different people have differing views on information security, and they tend to vary widely in their knowledge of the different subtopics. Frequently, these disparities lead to inadequate overall management. In large companies, information security audits are often performed in connection with financial audits.
In Small and Medium Sized Enterprises (SMEs), the level of information security often depends crucially on the requirements dictated by the large companies and customers they do business with. Suppliers and sub-contractors are increasingly granted access to companies' and customers' information systems. However, small companies usually do not have information that would require significant security procedures, apart from personal data that must be protected under the law.

The most common way companies increase information security awareness is to formulate an information security policy. Some companies have had their information security functions certified according to the BS7799 standard. Publishing information security certificates promotes wider awareness of information security. [36]

[36] FICORA Report

II. Legal landscape

As early as 1997, the Ministry of Finance and the University of Lapland jointly conducted a basic study concerning the drafting of information security legislation. [37] In 1998 they concluded that there was no need to enact a separate information security act.

There are, however, many laws involving information security that are aimed at specific groups such as telecommunications operators, the health care sector, or government. The provisions of these laws are mainly technology-independent and focus on the essentials: data and the means of safeguarding it. The harmonisation of legislation in the EU and certain international agreements are creating a need for new provisions.

Even so, there would be certain benefits if Finland had a general act covering information security. Such an act would raise social awareness of and interest in information security. Whether or not there is a general act, information security should be considered in all legislation. [38]

From the perspective of privacy, the Constitution Act of Finland, in section 8, protects the private life, honour, and home of every person; while prescribing that a data protection law will be developed by Parliament. In 1987 the Personal Data File Act was enacted by the parliament; and later updated to be made consistent with the EU directive in 1999 under the Personal Data Protection Act.

The updated act requires informed consent and informational self-determination, while the previous act only considered the use and disclosure of information. The law does not apply to processing of personal data for a private or purely personal use; or used by the media and arts. A separate piece of legislation articulates the exemptions to the Act for defense and public security.

Separate regulations have been implemented by the Finnish government applying to data held by the police in criminal information systems, medical information held by the national health service, passport information, and motor vehicle registers. There are some alarming developments as a result, however. For example, according to a 1999 law, when fining traffic violators, police may use their cellular phones to access official tax records of the offenders to assist in deciding the appropriate (and presumably proportionate) fine.

Two major laws govern the corporate sector. First, the personal data act implements the protection of private life and the other basic rights which safeguard the right to privacy in the processing of personal data. It also promotes the development of and compliance with good processing. Second, the act on data protection at work incorporates general provisions relating to data protection. These are also applied as they relate to working life. In addition, there are a number of mutually complementary provisions associated with data protection in working life, such as fundamental rights, labour law, the law on civil servants, law on safety at work, and criminal law. [39]

[37] Tietoturvallisuus ja laki. Näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä. University of Lapland, 1997

[38] FICORA report

[39] http://www.mol.fi/english/working/dataprotection.html

Special rules apply for telecommunication service providers. They are required by both Finnish and EU law to inform their users of any network security risks and any corrective action necessary. [40] Internet service providers are required to inform their users of computer viruses, data break-ins and other information security risks related to the Internet. They are also required to inform their users how to protect themselves against risks and what this would cost. [41]

A number of authorities are involved in helping interpret the laws on processing data. The Data Protection Ombudsman and the Office of the Data Protection Ombudsman provide guidance and advice on all issues related to the processing of personal data and control the observance of the law. The Office of the Data Protection Ombudsman is an independent authority operating in connection with the Ministry of Justice. The office is run by the Data Protection Ombudsman, appointed by the Council of State for a term of five years. Reijo Aarnio has been the Data Protection Ombudsman since November 1, 1997. The total number of staff is 18.

The Objective of the Office is to maintain and promote the right to privacy, one of the basic rights of each citizen, by:

- fulfilling the duties assigned to the Data Protection Ombudsman by legislation
- monitoring data controllers aiming at preventing violation of privacy in advance
- consulting private sector, authorities and courts of law
- promoting and educating good data processing practices
- assisting and supporting the development privacy enhancing technologies

The primary duty of the Data Protection Ombudsman is to ensure, in advance, compliance with the legislation concerning the keeping of registers. The Office of the Ombudsman provides information on the Personal Data Act that is aimed at both controllers and data subjects. Moreover, the in-house experts give lectures at seminars arranged by both the Office of the Data Protection Ombudsman and other organisations. The office also gives advice by telephone. The guidance and consultation relating to various data system projects is a task field which is important and constantly growing.

[40] Directive 97/66/EC, Article 4.

[41] Act on the Protection of Privacy and Data Security in Electronic communications (565/1999)

In addition to general guidance, the Data Protection Ombudsman provides controllers and data subjects with guidance and advice on request, and makes decisions pertaining to the compliance with legislation and implementation of the rights of data subjects. In matters concerning the implementation of the right of verification and the correction of personal data, the decisions of the Ombudsman are binding and subject to appeal.

Supervision is carried out through the controller's statutory duty of notification. However, even notable exceptions may be accepted within the limits of the Data Protection Directive. Inspections aim at assessing compliance with the

data processing laws, guiding controllers, improving the standard of systems, and preventing violations.[42]

If guidance and advice have failed to remedy a given situation, the Data Protection Ombudsman may, in certain cases, submit an act of violation for consideration by the Data Protection Board.

The Data Protection Board consists of a chair, deputy chair and five members, who are required to be familiar with register operations. The Board is appointed by the Council of State for a term of three years. The Data Protection Board processes and makes decisions on issues falling within its scope of action as defined in the Personal Data Act. At the request of the Data Protection Ombudsman, it provides regulations concerning the processing of personal data. In addition, the Data Protection Board may grant controllers permission to process personal data, provided that certain prerequisites are fulfilled.

The Data Protection Board deals with issues that are of principal importance in the implementation of the Personal Data Act. It also monitors the need for legislation concerning processing personal data and issues initiatives it deems necessary.

The Ministry of Finance is responsible for watching over information security in government IT systems. The Ministry of Finances Steering Committee for Data Security in State Administration (VAHTI) has published a number of instructions and recommendations to increase information security at agencies and government departments. The VAHTI instructions also make use of and disseminate universal information security instructions and practices. Application of these directi-ves could be increased in that part of the public sector outside central government, too. The Steering Committee for Data Security in State Administration (VAHTI) and the Ministry of Finance have been publishing information security recommendations and other information security material for 20 years.

[42] http://www.tietosuoja.fi/1560.htm

Finally, the Finnish Communications Regulatory Authority (FICORA) is a general administrative authority for issues concerning electronic communications and information society services. Its mission is to promote development of the information society in Finland.

FICORA also has duties concerning the protection of privacy and data security in electronic communications and is, among other things, involved in COMSEC (communications security) work. The aim of the COMSEC work is to ensure reliable telecommunications security that promotes the supply of content and services via network communications for the benefit of the information society. FICORA also has a role in CERT (Computer Emergency Response Team) activities to detect and resolve data security infringements.

The COMSEC functions aim to ensure the protection of communications privacy for network users and the security of communications networks. FICORA provides information and guidelines on communications security such as secure electronic services and reliable operation of certification service providers. FICORA also informs about risks relating to information security, with the aim of enhancing the use of encryption methods.

FICORA supervises protection of privacy and information security within the operations of tele-com-munications companies that provide public telecommunications services, and issues tech-ni-cal regulations and guidelines. FICORA controls that the telecommunications operators are prepared for emergencies and that they inform the users of telecommunications services about information security risks and measures for their prevention.

The Act on Electronic Signatures, in force as of Februray 1, 2003, gives electronic signatures created with specified methods the same status as handwritten signatures. FICORA's duty here is to supervise the certification authorities providing qualified certificates for electronic signatures. [43]

[43] FICORA report

III. Transformations in Policy and Technology

Every Finnish citizen is given a personal identity number. The personal identity number can be obtained from the Local Register Office. The ID is used for identification purposes, for example in banks and hospitals as well as in the registers of different authorities.

The personal identity number is a series of numbers consisting of the person's date of birth, individual number, and a control sign. The individual number differentiates persons born on the same day. The individual number is uneven for men and even for women. The control sign is either a number or a letter.

EXAMPLE: personal identity number 131052-308T

131052 = date of birth (date/month/year)
308 = individual number (even number = for a woman)
T = control sign

The electronic identification card is a secure network key for all on-line services which require personal identification, such as all government and many private sector services. It enables service providers to reliably identify users. The card is also an official travel document for Finnish citizens in 19 European countries. It costs 29 and is valid for three years. This period was chosen for security reasons. As computing power is constantly increasing, nobody can predict how long the currently embedded 1024-bit RSA key will be secure. Three years was selected as a suitable compromise between usability and security.

The electronic identification card is issued by the local police department. The Finnish Population Register Centre supplies the on-board certificates which are used in electronic identification. In addition to the card, a card reader is needed for on-line use. In the future, identification will be available from mobile devices such as a cellular phones equipped with a special chip.

In addition to technical data, the card contains three certificates: the cardholder's authentication certificate, the cardholder's digital signature (non repudiation) certificate, and PRC's CA certificate. The cardholder's certificates contain only the first and last name of the holder and a unique electronic user ID (FINUID). The chip does not contain the personal identification number issued at birth, nor does it contain home address, date of birth, and so on. The electronic user ID is a sequential number with a control sign at the end. Unlike the personal identification number, the electronic user ID does not reveal any information about its holder. The electronic user ID never expires.

The directive on electronic signatures is in force in the EU, and member states are obliged to adhere to it. Banks and financial institutions, for example, have already begun to build on-line services where a digital signature is as valid as a traditional signature. Therefore, the law which puts the directive into effect only clarifies an already existing situation. For public administration, there is already a law in effect (The Act on Electronic Service in the Administration) which states that a digital signature is valid in all public administration on-line services. [44]

[44] See http://www.sahkoinenhenkilokortti.fi. More information can be obtained from the manufacturer's website: http://www.setec.fi/english/identification/eid/index.html

RFID and Mass Transit Travel Card

VTT Technologies, a government research centre, has developed a new type of high frequency (900 MHz) RFID tag that can be read with a transceiver up to four meters away. The signal can also penetrate obstacles. VTT experts believe that these Radio Frequency Identification, or RFID tags will be commonplace within ten years.

RFID technology already has a number of industrial applications in Finland. For example, the paper industry uses these types of electronic tags to identify large rolls of paper. Research professor Heikki Seppä at VTT believes that these small devices will have a major impact on people's everyday lives in the years to come. He predicts that demand for tags will be in the hundreds of billions.

RFID technology would allow customers to find out even before entering a shop if the goods they need are available there. Eventually there could be stores without checkout clerks. All purchases would be recorded electronically and charged to the customer's account without the customer's having to take them out of the shopping cart. In the home, RFID technology would make it easier to trace misplaced objects.

In the Helsinki region, the most familiar application of RFID technology is the new travel cards that are replacing paper tickets in the area's public transport system. The partners in the project are Helsinki Metropolitan Area Council (YTV), Helsinki City Transport (HKL) and the railway company VR.

The use of travel cards is recorded in a database. This information can be accessed to aid transport capacity planning. The movements of travel card users are saved and can be accessed for later retrieval. The data from the transport system has been used for crime investigations in serious cases.

YTV records the customer information it needs in order to take care of the customer service and consumer protection in the Travel Card System. The information is used in cases such as delivering personal Travel Cards, changes to the customer's contact information and municipality of residence, returning lost Travel Cards to customers, putting a lost Travel Card on a revocation list, terminating customer connections.

On request, the personal data or business ID of the owners of multi-user Travel Cards can also be recorded in the

system. Personal data/business IDs may be transferred to outsiders only when the law or orders of the authorities call for it. YTV and municipal service points' employees and the persons in charge of the system have the right to browse and update the customer data recorded in the system. The aforementioned persons also have the right to browse the data stored in the central processing unit concerning the travel periods and value a passenger has loaded into his/her card, as well as the data on how the value stored in the card has last been used. It is not possible to browse the travel data at the point of service. [45]

The travel card received heavy public criticism after its introduction since it was theoretically possible to connect traveller's IDs with travel route information. After the Data Protection Ombudsman made the issue public, YTV changed its policy.

IV. PETs in Finland

As you'd expect from a country that nurtured a high-tech company as large as Nokia, Finland is home to a number of interesting security companies. What follows is a brief guide to their products.

F-Secure [46] develops different anti-virus, file encryption, network security, and handheld security software. Most F-Secure products run on standard PCs for all major platforms from desktops to servers and from laptops to handhelds. The company claims to support businesses with a broad range of centrally managed and up-to-date security solutions to enable a truly mobile enterprise.

[45] See http://www.rafsec.com/ and http://www.idesco.fi for more information on RFID and http://www.matkakortti.net/english/index.html for more information on travel card.

[46] http://www.f-secure.com

Miotec [47] develops smart cards and chip technology-related software. Miotec supplies international telecommunications operators with, for example, memory cards or scratch cards to be used as prepaid phone cards. Miotec also develops and produces microprocessor chip cards for secure electronic transactions. Miotec's contactless cards are used in logistics, identification, and ticketing applications. Technologies like RFID and PKI can be combined into a single card which can serve in systems for access control, working time control, and securely logging on to an information network. The MioCOS card operating system developed by Miotec enables a variety of designs for PKI and biometric cards. Its modular structure also underlies the Miotec products developed for the mobile environment.

Secgo [47] claims to offer solutions for secure remote access for employees, secure extranets for customers and partners, secure WLANs, mobility management, secure networking and monitoring of gaming, recycling and vending machines, and highly secure military and governmental networks. Secgo's solutions are widely used in demanding business sectors such as government, banking and finance, service provider, manufacturing industry, and the military.

Secgo also provides the first solutions in the field to fulfil all the standards and recommendations for the open digital trunked radio standard TETRA. Defined by the European Telecommunications Standardisation Institute, TETRA is designed for the most demanding professional networks, such as those belonging to official and public authorities. Started in 1994, TETRA is now widely established with more than 30 operational networks and nearly 100 contracts worldwide. Secgo is responsible for developing and supplying the AKD (Authentication Key Distribution) solutions that will ensure the required high level of security for the network.

Setec [47] develops and manufactures SIM card solutions that provide secure electronic identification for leading telecom operators around the world. The company's new eSIM 3G, for example, is a new SIM card for 3G mobile networks (UMTS). As Setec's new card complies with both GSM and 3G requirements, all mobile services offered today can be accessed with it. It uses PKI technology. In addition, because the card has both full and application toolkit support, operators can design and implement secure services such as m-commerce and m-banking as well as information, entertainment and gaming services.

[47] http://www.miotec.fi/

[48] http://www.secgo.fi/index.html

[49] http://www.setec.fi/

SSH Communications Security [50] is a de facto Internet standard for secure remote connections developed by SSH Communications Security. SSH Secure Shell is an application that protects TCP/IP connections between two computers; it is often used as a secure version of Telnet. The connection is encrypted on the application layer, which means that the security provided by SSH is available regardless of the network connection speed or type. SSH is client-server software, so the client is always the initiator of the secured connection and the server is always the respondent.

[50] http://www.ssh.com/

V. Other issues

The majority of users are unaware of the risks of new tech-

nology or, in some cases, overestimate them. Examples of the latter are fears related to ordering and making payment online. The situation is partly due to the rapid changes taking place in the significance of protecting data and privacy. Also the media has given considerable publicity recently to information security offences, prompting many people to realise the importance of information security.

The importance of terminal devices in information security may remain unclear to the user. Users are not aware of the information security implications of devices and Internet connections when they buy them, and do not appropriately appreciated their information security properties. This is probably the greatest information security threat to the private individual, particularly because it concerns companies too. A lost device may contain business secrets, passwords, or other confidential information.

Lately, consumers have criticised Internet service providers for not providing as high a level of information security for Internet connections and services as they could. Service providers are considered to have concentrated too much on product features in marketing, leaving information security publicity to the statutory minimum. It has been for example suggested that firewalls preventing crackers from operating should be a standard security feature that customers should be entitled to expect in Internet products. Consumers should not, according to public opinion, be expected to take responsibility for something that they cannot be realistically expected to be able to manage.

As a whole, information security training is lacking in the Finnish education system. Such training as there is focuses on technological issues, and there are not enough courses. The presence of information security in the news and elsewhere in the media has increased general awareness of information security, albeit primarily from the point of view of risks. Various help material is available for users: a citizen's information security guide produced by the Finnish Information Society Development Centre (TIEKE), the Ministry of Finance instructions aimed at users, among others, (email, virus protection, and so on), electronic and printed material distributed to customers by service providers and virus protection companies, and various courses and other training in information security. [51]

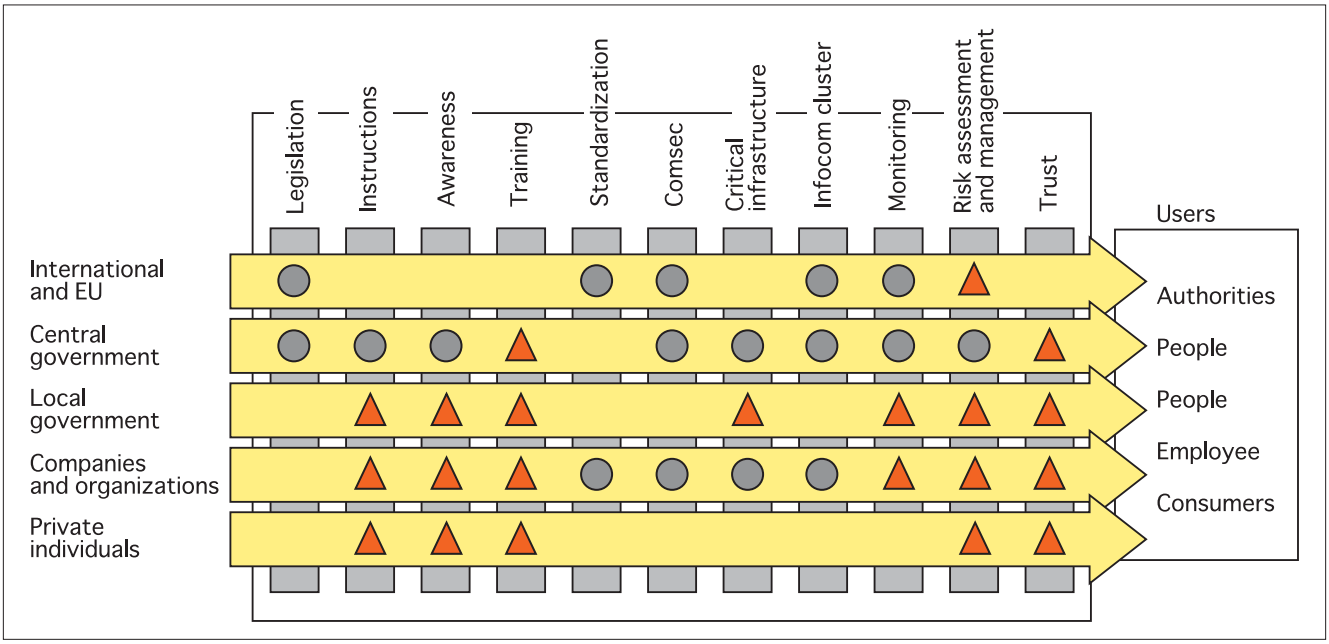
[51] FICORA report

VI. Implications and Conclusions

Based on the Finnish experiences our recommendations for future public policy on privacy issues:

- Take into account the opinions of all sectors of the society that are affected by the privacy policy. Especially critics in the citizens' sector have voiced their desire for more transparent policy formation.
- Take extreme care in connecting personal information to information databases. For example, in public transportation it is unnecessary to connect the ID of a traveller to information gathered for uses such as traffic volume measurement and route optimisation.
- Implement privacy technologies that are easy to use and affordable. For example, the national ID card in

Figure 1. Strong functions (circles) and needs (triangles) in information security as identified in FICORA's Report (p28). INFOCOM = IT and telecommunications.



Finland has not become popular because it requires expensive additional hardware and its use requires extra learning.

- The impact of data protection ombudsman as a specialised government expert on privacy issues with executive powers has been very positive. Data protection ombudsman and his office have become respected authority.

Privacy Enhancing Technologies in France [52]

I. Introduction

The right to privacy was first recognised in France in the mid-19th century, and was added to the Civil Code in 1970. This privacy right is not explicitly included in the 1958 Constitution, but the Constitutional Court ruled in 1994 that it was implicit. [53]

In 1974 the French political scene was shocked by the discovery of a government project (code-named SAFARI) aimed at unifying citizens' different IDs into a single identifier. This project was attacked by civil libertarians, who denounced it as "la chasse aux français" ("the hunting of the French"). This scheme would have led to massive cross-departmental sharing of all administrative databases. [54] The resulting scandal helped the French Parliament to pass a strong law protecting privacy from public and private abuse, the Data Protection Act (Loi Informatique, aux Fichiers et aux Libertés [55]). This law created the Data Privacy Commission (CNIL), which was set up in 1978.

Since then, the French Republic has effectively resisted attempts to create "bridges" between databases; with some exceptions. In 1998, for example, the Parliament gave the tax authority the right to access personal data from the Social Security system in certain circumstances. The CNIL gave its approval to this scheme a year later [56], but observers have always considered this exception to be a fundamental contradiction to the spirit of the Data Protection Act.

This very sensible "non-crossing" principle has always been kept in mind when thinking about e-government projects. The dream of "Administration électronique", which first emerged with the Internet revolution in 1995, is still tied by this fragile consensus between easing citizens' access to administrative information and the "non-crossing" principle.

There are two other cultural phenomena that are important in understanding France's situation with respect to privacy and privacy-enhancing technologies.

First, France has traditionally seen cryptography as something that should be owned by the government. In general, the government has seen no reason why algorithms should be open and has insisted on a system whereby the government maintains control of keys. Even now, a licence is required for certain types of strong cryptography.

Second, smart cards have a long history in France. Credit cards in France have used a chip inside that requires a PIN code for more than two decades.

[52] Jerome Thorel.

[53] The 2002 Privacy and Human Rights report, by EPIC & Privacy International http://www.privacyinternational.org/survey/phr2002/

[54] Le Monde du 21 mars 1974, "SAFARI ou la chasse aux français".

[55] Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés": http://www.cnil.fr/textes/text02.htm

[56] CNIL recommendation about the social security & tax decree http://www.cnil.fr/textes/text084.htm

II. Legal landscape

As a member of the EU, France should have amended the Data Protection Act in 1998 in order to implement the European privacy directive 95/46/EC in national law. France has missed the deadline twice and made no significant progress on this matter in 2002 because of political elections. In July 1999 the EU Commission in Brussels took legal action against France and eight other member states for this failure. France was also in the January 2000 list of five member states that failed to implement another privacy directive (97/66) specifically covering electronic communications.

The former socialist government (July 1997 to April 2002) began to prepare a bill to amend the Data Protection law in August 1997, but after a Parliamentary report issued in March 1998 the bill was frequently postponed during legislative sessions. The draft bill was adopted by the Council of Ministers on July 18, 2001 and passed the first reading by the National Assembly on January 30, 2002. [57] The bill has moved to the Senate since then, and is scheduled for debate later in 2003.

[57] "Projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978": http://www.assemblee-nat.fr/dossiers/cnil.asp

The bill would give the CNIL more power over commercial data processing and allow it to impose fines (from 1 to 150,000) for abuses, and would strengthen individual right of access and correction. However, it would weaken the Commission's control over large government information systems and new databases known as "fichiers de souveraineté". These are defined to include databases relating to the safety of the State, defence, public security or the penal system. Such systems include police records like the judiciary police database STIC (Systeme de traitement des infractions constatées). This is an initiative by the Minister of the Interior to merge multiple police reports including victims and suspects' names. These include people who have never been convicted of any crime. STIC also includes the French parts of EU-wide data and biometric files of illegal immigrants and political asylum seekers (SIS - Schengen Information Systems, and Eurodac). The CNIL will no longer have the power to review the governmental decrees that would create such systems. This revision is thought to be a response to the difficulties experienced by the government

in implementing the STIC. The system was first envisioned in 1995 but was not implemented until July 2000 following the reluctant approval of the CNIL. [58]

The current right-wing government has approved recent amendments to its domestic security legislation (Projet de loi pour la sécurité intérieure PLSI) to create a special "right of access and correction" for these "sovereignty files". [59] Along with this development, however, further amendments were included, some more problematic. The first reading by the Assembly added a provision that allows law enforcement agents to request transaction records, traffic data, and subscriber data through the use of an electronic warrant. This form of warrant would allow for a "remote search", rather than having the police present themselves physically at service providers; and may result in a significant increase in such requests from Internet, mobile and fixed telephone operators, banks and any private sector database in order to identify a customers and subscribers.

The projects of Interior and Homeland Security Minister Nicolas Sarkozy are more ambitious regarding cross-sharing of law enforcement files. He wants to allow mutual access to the STIC and JUDEX, the equivalent for use by the gendarmerie (the other judiciary police branch, although gendarmes have military status). The PLSI would allow mere administrative agents to access these databases to check the morality of would-be candidates for security jobs, passport and visa requests. These are among the provisions approved by MPs in first reading on Jan. 28, 2003. [60]

The CNIL opposed the project, explaining that it would raise "important concerns regarding privacy rights of individuals". [61] Among the threats: the number of authorised people who could access these files may go up tenfold from today's approximately 40,000 (police and gendarmerie officers). In January 2003, La Fédération Informatique et Libertés, a group of civil society NGOs, published a list of flaws found in the STIC after CNIL verfications. According to their figures, between 20 and 25 percent of the system is flawed. [62]

[58] Privacy and Human Rights report 2002

[59] Projet de loi pour la sécurité intérieure, National Assembl' Law Commission's report, 18 December 2002: http://www.assemblee-nationale.fr/12/rapports/r0508.asp

[60] Projet de loi pour la sécurité intérieure — 1st reading, January 28, 2003: http://www.assemblee-nat.fr/12/ta/ta0079.asp

[61] Position de la CNIL sur le PLSI — "fichiers de police judiciaire et fichier national automatisé des empreintes génétiques", 24 octobre 2002

[62] Les erreurs du STIC, Federation informatique et libertés FIL,11 janvier 2003: http://www.vie-privee.org/comm99

The PLSI also requires the inclusion of suspects for even small crimes in the 1998 DNA database. The goal: a million people in the coming years, following the UK example. [63]

The following list presents the other laws with the most significant implications for privacy.

- *Email and phone surveillance (content): a 1991 Act (n° 91-136, 10 July 1991) regulates the wiretaps requested by the government's secret services (mainly national security and terrorism cases) under the surveillance of an independent Commission (CNCIS); the Judiciary can also request investigative tapping under the control of the Justice's High court (Cour de Cassation). Electronic mail has always been affected by the 1991 law, without the need for amendments. However, in 2003 the government should take legislative steps to adapt wiretaps to the digital age.*
- *Video-surveillance: no clear regulation existed before a 1995 Act (n°95-73, 21 January 1995) implemented by decree in October 1996; any system must be declared to the State Prefet and the CNIL has a very limited control over public video systems.*
- *On November 15, 2001, the Parliament enacted the Loi sur la Sécurité Quotidienne (LSQ), a legislation in which new anti-terrorism provisions were added, in direct response to the September 11, 2001 terrorist attacks. The enacted law includes provisions on data retention and compelled access for the government to cryptography keys. In the first instance, Internet Service Providers and telecommunications companies now are compelled to record and store traffic and location data of their subscribers for a period of maximum one year. By adopting this provision France was ahead of the EU Directive 2002/58 of 12 July 2002, on privacy and electronic communications (which replaces the 1997/66 directive), that establish the data retention principle. Regarding the second instance, encryption rules in France are among the most complex and user-unfriendly. New rules in 1999 state that encryption is "free to use" but any use of keys longer than 128-bits in length requires a declaration and licence, and for providers authorisation is required. (12). The 2001 LSQ added the last modifications to the encryption regime: to create a cryptanalyst task force for lawful access to encrypted mail, and a "government access to keys" scheme, that considers a crime not to give access to decryption keys requested by a judge warrant- for software and service providers as well as individuals (13). Cryptography rules will change this year according*

to provisions included in the "digital economy bill".

[63] PLSI - L'ere du soupçon, 10 dec 2002: http://www.vie-privee.org/news55

III. Transformations in Policy and Technology

The PLSI, set to be approved in March 2003, is only one of a long list of legislation being prepared to tackle the information society and comply with recent EU directives. These include a telecommunications package, a digital economy bill ("Projet de loi pour la confiance dans l'économie numérique"), the supporting legislation for the European Copyright Directive ("Projet de loi de transposition de la directive européenne sur le copyright EUCD"), and the ongoing bill on combating serious crime ("Projet de loi de lutte contre la grande criminalité").

Electronic administration and e-government

France has pursued numerous initiatives related to the "administration électronique". However, these primarily consist of commissioning white papers ("livres blancs"), "reports", and "recommendations". Requested by the government, these are written by legal experts, civil servants, and parliament members. Since the first one in 1998, a total of 20 reports has been produced. [64]

In 1998, the task of electronic administration was thought of as a way to modernise often outdated public infrastructures and computer systems. As the first rapporteur, Jean-Paul Baquiast, noted,

"l'État, tel que nous le concevons en France, doit pour évoluer maîtriser complètement Internet, clef de la société mondiale de l'information. Celle-ci impose à l'État des contraintes qu'il doit surmonter. Elle lui ouvre en contrepartie des opportunités de rajeunissement et de développement qu'il doit saisir. C'est donc bien l'avenir de l'État et de ses administrations qui est en cause." [65]

[English: "The State, as we conceive it in France, in order to evolve must completely grasp and master the Internet, which is the key to the global information society. This imposes on the State constraints that it must surmount. It opens in return opportunities for rejuvenation and development that the State must seize. This is definitely the future of the State and its administrations that is at stake."]

The last rapporteur, Pierre de La Coste in his study "Hyper-Republic", written at the request of the under-secretary for State Reform, introduces his work as follows:

"Les problèmes posés par l'administration électronique sont presque uniquement de nature sociologique, voire culturelle. Mieux : tout problème prétendument juridique ou technique (lié à la sécurité sur Internet ou à la signature électronique, par exemple) n'est en fait que le masque d'un problème sociologique, tenant sim-

Figure 1: Timetable for e-government in France

	Description	Etat	Points de blocage	Solutions	Calendrier
Premier niveau	Mise a disposition d' information statique	Pratiquement acheve	Grandes difficultes de mise a jour des informations anciennes - manque de structure de l'info	Moderniser l'infrastruscture et l'organization de production des site administratifs	1996-2004
Deuxiéme niveau	Mise a disposition d' information utilisables	En voie d' achevement	Nombre, complexite ou absurdite de certains formulaires papier	Supprimer, simplifier	1998-2004
Troisiéme niveau	Teleprocedures Teleservices	En course	Pieces annexes Manque d'interoperabilite Signature electronique	Regrouper par familles de teleprocedures Passer a l'etape suivante	2000-2005
Quatriéme niveau	Decloisonnement	En projet	Protection des donnees personnelles	Contrat de confiance Communication	2002-2012

plement à l'antagonisme entre la tradition administrative française et la nouvelle culture du réseau.

"Enfin ... le management de l'informatique publique n'a guère évolué depuis une dizaine d'années et le rapport du commissariat général du Plan sur l'informatisation de l'Etat de 1992. Ainsi, la responsabilité des systèmes d'informations est très rarement attribuée au niveau d'une direction, elle échoit au mieux à une sous direction, voire à un simple bureau, ce qui empêche souvent que les problématiques liées aux systèmes d'information soient portées fermement au niveau du comité des directeurs." [66]

[64] Les rapports de l'Administration électronique: http://www.men.minefi.gouv.fr/webmen/informations/rapports/rapp_ae.html

[65] "Propositions sur les apports d'Internet à la modernisation du fonctionnement de l'Etat", Jean-Paul BAQUIAST — rapport au Premier ministre.1998.

[66] "L'Hyper-République — Bâtir l'administration en réseau autour du citoyen", rapport au secrétaire d'Etat à la Réforme de l'Etat, 8 Jan. 2003: http://www.internet.gouv.fr/francais/textesref/rapdelacoste/hyper-republique.PDF

[English: "The problems posed by electronic administration are almost completely social and cultural. Better stated: all problems that seem to be legal or technical (linked with Internet security or digital signatures, for example) are in fact only masks for social problems, having to do simply with the antagonism between traditional French administration and the new network culture.

"Really … the management of public information has hardly evolved in the last decade since the Commissioner General's 1992 report on the computerisation of the State. Therefore, the responsibility for information systems is only very rarely placed at management level; it usually falls under lower-management levels, indeed often a single department, which often prevents news of the problems related to these systems from being brought to the attention of boards of directors.]

The first "national plan for the information society" was released in 1998 by PM Lionel Jospin (PAGSI, "Préparer l'entrée de la France dans la société de l'information"). The most recent is the RE/SO 2007 plan launched by Prime Minister Jean-Pierre Raffarin in 2002 [67]. In between these two stages, e-government has indeed become a reality if you go by the number of regulations, decrees, "arrêtés" or "circulaires" to ease electronic communications use and legitimacy / recognition in public services. [68]

For example:

- *Décret no 98-1083 relatif aux simplifications administratives; (decree on reducing administrative red-tape)*
- *Circulaire relative à la diffusion de données juridiques sur les sites Internet des administrations; (circular on the dissemination of legal data on government websites)*
- *Circulaire(s) et décret(s) relatifs à la "simplification des formalités et des procédures administratives". (circulars and decrees relating to the simplication of formal administrative procedrues)*

But these measures are not very citizen-oriented (the exceptions are explained below). They have been aimed primarily at legalising digital procedures, especially regarding electronic signatures for certifying business contracts.

Examples:

- *Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (law on the technological verification procedures for digital signatures)*
- *Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique [69]: (decree on adapting the Civil Code for digital signatures)*

In August 2001 a decree created the Agency for Information Technology and Communications in the Administration, ATICA (l'Agence de Technologies de l'Information et de la Communication dans l'Administration) and placed it under the supervision of the Prime Minister's office. It is dedicated to coordinating projects inside government services.

Under the new RESO plan of 2002 this agency will become the AAE ("Agence pour l'administration électronique"). The AAE will have more responsibilities. These will include conducting policies to ensure the integrity and security of electronic public services and also deploying privacy-enhancing technologies, as recommended by the January 2003 e-government report.

In August 2001 a decree created the Agency for Information Technology and Communications in the Administration, ATICA (l'Agence de Technologies de l'Information et de la Communication dans l'Administration)

and placed it under the supervision of the Prime Minister's office. It is dedicated to coordinating projects inside government services. [70]

Under the new RESO plan of 2002 [71] this agency will become the AAE ("Agence pour l'administration électronique"). The AAE will have more responsibilities. These will include conducting policies to ensure the integrity and security of electronic public services and also deploying privacy-enhancing technologies, as recommended by the January 2003 e-government report. [72]

[67] RE/SO 2007, http://www.internet.gouv.fr/francais/textesref/RESO2007.htm

[68] Ressources utiles concernant l'Administration électronique: http://www.men.minefi.gouv.fr/webmen/informations/rapports/ress_ae.html

[69] Decree on electronic signature:http://www.legifrance.gouv.fr/texteconsolide/ARHCG.htm

[70] ATICA Decree — 22 août 2001 portant création de l'Agence pour les technologies de l'information et de la communication dans l'administration: http://www.legifrance.gouv.fr/texteconsolide/PRHGY.htm

[71] RESO plan, Ibid note 4.

[72] Hyper-Republic report, Ibid note 3.

E-government in practice

On February 6, 2003 the European Commission released the results of its third semi-annual study of the quality of e-government services in 18 countries (15 EU members plus Norway, Iceland and Switzerland). The EC, which wants to assess the impact of its eEurope initiative, "defined a common list of twenty basic public services to be analysed, divided into 12 citizen-oriented and eight business-oriented services." [73]

By the standards of this study, France would be listed on average in Stage 2, "One-way Interaction" services. Other classes on the list: Stage 0 "Development"; Stage 1 "Information"; Stage 3 "Two-way Interaction"; Stage 4 "Transaction", meaning full electronic case handling.

The tax authority, DGI (Direction générale des impôts), is the exception. In 2001 it set up "TELE-IR", an "electronic declaration of revenues", in which people could submit tax returns without writing on paper at all. Between March 11 and 25, 2002, the service recorded 115,149 on-line declarations, seven times more than in 2001. Around 150.000 people downloaded digital certificates to identify themselves to the DGI and access its "dossier fiscal". Certificates are valid for 3 years. More than 100,000 consultations of private tax files had been carried out by March 29, 2002. The DGI opened a second service in 2002, with a "Stage 4" procedure that allows people to actually pay their taxes via e-certificate. [74]

Another experiment, launched in 2001 by the DGI, allowed the remote declaration of Value Added Tax collected by private-sector companies. (VAT registration is mandatory for those with revenues of 15 million or more). This "TELE-TVA" scheme also allows corporations to pay their annual VAT electronically. Two network systems are available: the "electronic form exchange" (EFI), and the more traditional "electronic data exchange" (EDI). Proposed for the first time on May 1st, 2001, TELE-TVA may be used by potentially 3 million corporations that must generate around 16 million tax declarations each year. The network is secured by protocols used by French private and public banks. [75]

[73] eEurope - Egov barometer: http://www.europa.eu.int/pol/infso/index_fr.htm

[74] Tax authority portal http://www.impots.gouv.fr

[75] TeleTVA description, technical protocols, key facts: http://www.impots.gouv.fr/documentation/pratique/teletva/plaquette2.pdf

Regarding this scheme, the EU Commission study on e-government policies states [76]:

> *"Les services qui conservent la meilleure performance sont les services générateurs de revenus (principalement impôts et contributions sociales). La France compte parmi les 5 pays atteignant la note maximale de 100 %, correspondant au traitement intégral du cas en ligne (enregistrement, décision, remise, et paiement le cas échéant)."*
>
> *[English: "The services that show the best performance are the services which generate revenue (principally taxes and social contributions). France is one of the five countries that attained the highest rating of 100 percent as a result of its entirely online processing of cases (registration, decision, submission, and payment when owed).]*

The no-crossing principle

When the "no-crossing" principle is applied to e-government projects, public debates have emerged in the last couple of years.

In November 2000 France entered a new phrase in government-to-citizens electronic interaction: the creation of the Web portal "service-public.fr". [77] Dedicated as a single resource point for all official documents and legal "formulaires", this project is scheduled to become a personalised portal for citizens' relationships with public services (mon.service-public.fr). As the decree from November 15 of that year states [78]:

"Un site personnalisé "mon.service-public.fr" sera proposé d'ici à 2005 à chaque usager pour lui permettre de gérer en ligne l'ensemble de ses relations avec l'administration. L'ATICA est chargée de mener, d'ici à mars 2002, une étude technique préalable de ce dispositif."

[English: "A personalised "mon.service-public.fr" will be offered some time between now and 2005, which will allow for each user the ability to manage, on-line, all of his interactions with the government. ATICA is responsible for conducting, from now until March 2002 a preliminary technical study of this system.]

[76] Ibid note 3.

[77] Arrêté du 6 novembre 2000 relatif à la création d'un site sur internet intitulé "service-public.fr" : http://www.legifrance.gouv.fr/citoyen/jorf_nor.ow?numjo=PRMX0004473A

[77] Decree monservicepublic.fr: http://www.fonction-publique.gouv.fr/reforme/cire/2001/cire_index.htm

Because of the post-September 11 context – that is, anti-terrorist legislation, including the November 2001 Loi sur la Securite Quotidienne (LSQ) – the government felt it needed brand-new privacy guidelines. The then minister for Public Services and State Reform, Michel Sapin, launched a public debate. He consulted a group of legal experts led by the président honoraire de la Cour de cassation (France's highest court), Pierre Truche, and asked this group to write a white paper on how to resolve privacy with the fear of datasharing and indexing — the French paradox. Michel Sapin asks for a "new deal" on data privacy [79]:

"... l'État se donne pour objectif que soient proposées en ligne, d'ici à 2005, toutes les démarches administratives des particuliers, des associations et des entreprises, ainsi que les paiements fiscaux et sociaux. II s'agit d' ... accéder rapidement à toutes les informations administratives, effectuer en ligne et de manière sûre toutes ses démarches avec les services publics, retrouver l'historique de ses démarches passées et stocker en ligne, à son gré et en toute sécurité, les données administratives qui le concernent. ... La généralisation des téléservices publics implique de nouvelles formes de partage ou d'échange de données entre les administrations, et donc la définition de nouvelles règles ... qui devront naturellement s'accompagner d'une forte sécurité des données personnelles nécessaire à la protection de la vie privée."

[English: The state sets itself the objective for e-government: between now and 2005 all the administrative services and processes of individuals, associations, and enterprises, as well as fiscal and social payments. It's a question of moving rapidly to ensure that all personal information held by governments is on-line, reliable, and includes all its interactions with public services, including the ability to retrieve all previous transactions, and keep online, as they please all the relevant data of interest to the state … Mass deployment of public online services implies a new form of sharing of data within government, and therefore we need new rules that should naturally include a strong regime of data protection to ensure privacy.]

[79] "Administration électronique et protection des données personnelles", janvier 2002. http://www.ladocumentationfrancaise.fr/brp/notices/024000100.shtm

The white paper explores different policy directions and questions, including

- *the creation of personalised accounts and portals involving access controls such as through cryptography (and whether this should be using a single key or multiple keys), and/or using a national ID-card with a chip-system with digital certificates embedded within, as used in Finland and Italy. Also the white paper explores the idea*

Figure 2: September 2002 poll by FDI examining why 18 percent of those surveyed said they were against the creation of a "portal" basedon mon.service-public.fr

Confidentiality is too difficult to establish	60 percent
Threat of centralising administrative data, making it accessible to all state-owned services	28 percent
Concerned that it would allow identity theft	18 percent

- *the creation of a special right to be informed regularly (perhaps monthly) about the use and/or change of your personal data*

After Truche's white paper was published, a public on-line debate that was organised in 2002 by the a group Le Forum des droits sur l'internet (FDI) was resumed by the consultative body. [80] The main results from this process, regarding data privacy, include:

- *the proposals seemed to sacrifice the non-crossing principle;*
- *the "personal portal" project still badly feared by citizens;*
- *a veritable pact of confidence needed to be instituted … which could have its origins in a certain number of administrative reforms;*
- *a personal portal on-line incites a certain rereading of classical principles for protecting personal data.*
- *technical solutions for identification and security may rest hidden from the eyes of the public, with the exception of a tiny card.*

[80] On-line forum: http://www.foruminternet.org/forums/descr.php?f=7

The FDI's final recommendation supports the scheme "www.monservice-public.fr" and for a "PAP" ("portail administratif personnalisé"), but considers the possibility that the user could access the portal without having to have a single ID or digital certificate.

In a survey, FDI found that (see Figure 3) security and privacy was a significant concern. FDI did some research into why 18% of those surveyed said that they opposed the portal.

FDI recommended to the government that

- *data cross-sharing could occur only with consent, and with strict adherence to the 1978 law [81]:*
- *the administrative personal portal should be like a simple footbridge permitting the user, with the aid of hypertext links, to access different services of the administration and not like a single administrative account centralising all of the user's admnistrative details;*
- *the functioning of the personal administrative portal relies on a principle of voluntary use and reversibility;*
- *the personal portal project will be instituted and regulated by law;*
- *the rights of access and correction laid down by the law of January 6, 1978 will be provided in a manner such that these functions may be performed on-line;*
- *that changes be made to the 1978 law to allow for legal mechanisms that would require the reporting of interlinking between government files containing personal data*
- *and regarding the functioning of the personal administrative portal: it will be possible to use either a smartcard to identify oneself or through the use digital certificates.*

[81] Recommandation du Forum des droits sur l'internet, 03/02/2003: http://www.foruminternet.org/recommandations/lire.phtml?id=493

According to the latest reports, published in January 2003, the 'French paradox' is considered a major obstacle to the development of e-government. De La Coste thinks that "Big Brother" may change hands if the cross-sharing exception stays alive per se:

"...la question n'est plus de savoir si les fichiers de données personnelles seront exploités et croisés. La question est de savoir qui le fera : l'Etat lui-même ou bien le grand Editeur de logiciels qui a maladroitement donné à son grand projet de commerce électronique le nom d'un document officiel que ne délivre que l'Etat régalien ? ... Si l'Etat en France parvient à décloisonner son administration et à fonctionner réellement en réseau, si les Etats européens parviennent à former eux-mêmes un « réseau d'Etats en réseau », ils n'auront aucune difficulté...

"Dans le cas contraire il n'est pas impossible que se réalise le cauchemar Orwellien, mais pas sous la forme prévue par son auteur. Car les grands groupes qui détiendront les clés des technologies de l'information ne se priveront pas de décloisonner et de croiser à la place des Etats les informations personnelles qui tomberont en leur possession, et feront sauter les barrières juridiques dérisoires que ceux-ci tentent de leur opposer, notamment en France. Big brother, loin d'être à la tête de l'Etat, sera son pire ennemi." [82]

[English: … the question is no longer knowing if databases of personal information will be exploited and correlated. The question is knowing who will do it: the State itself, or rather the Great Software Producer who has maliciously given his great ecommerce project the name of an official document that delivers only what the State regulates? If the State in France came to

decompartmentalise its administration and function really by network, if the European States come to reform themselves as "network of States' networks" they will have no difficulty…

Otherwise, it's not impossible that the Orwellian nightmare will come about, but not in the form imagined by its author. Because big groups who release the keys to information technologies will not hesitate to decompartmentalise and to correlate personal information that falls into their possession on the State's behalf, and they will make it jump derisory legal barriers that dare to oppose them, notably in France. Big Brother, far from being the head of the State, will be its worst enemy.]

[82] Ibid note 3. Conclusion.

IV. PETs in France

Electronic certification and PKI

In 2002, 35,000 digital certificates were issued in France [83]. The major providers are private consortiums — IT sevices companies as well as established banks and credit institutions. All digital certificate issuers can also have the "trusted third party" status of 'Certification Authority' (CA).

The market leader is Certplus (Gemplus, France Télécom, Banques Populaires, Verisign), who have 75 percent of the market share. The TéléTVA tax procedure launched by the ministry of the Economy and Finance (Minefi) has been a strong catalyst for private sector providers. The CAs support the Minefi project include: BNP Paribas-Authority Entreprise, Certinomis (La Poste), Certplus, ChamberSign (Chamber of Commerce), Certigreffe (Commerce Tribunals), Click and Trust (Certplus), Banques Populaires, Crédit Lyonnais, SG Trust Services (Societe generale), Crédit Agricole, CCF-HSBC. [84]

Digital certificates are generally offered to companies, SMEs and certain professions like lawyers and physicians. But recent trends have been to market certificates to individuals. For example, Banque Populaire has been trying with its new CA called "Click and trust". Certigreffe, a system created by the Commerce Tribunals to secure business-to-business transactions, has decided to promote its system to the general public as well.

Encryption-based privacy enhancements

Computer security providers, especially foreign companies, have encountered some regulatory problems in developing encryption software "for the masses" in France. This is because of the complex rules imposed by the governement, as discussed above. For example, at key lengths above 128-bits, the regulatory burdens increase. Above that limit, encryption providers must always have an licence, like a gun dealer's permit, in order to sell its products (to corporate as well as individual clients).

Under the new LSQ law, passed late 2001 with antiterror provisions, every "confidentiality software provider" must keep all private keys in custody, in order to disclose a requested key to the police if a warrant is presented. Failure to disclose a requested private key could led to three years in jail and a fine of 45,000 [85]. This obligation is also placed on citizens that have been issued a warrant to provide access to an encrypted email. [86]

[83] Infrastructures à clés publiques: Certplus profite des hésitations de l'État, 01net, 13/09/2002, http://www.01net.com/article/193408.html

[84] Minefi references: http://www.finances.gouv.fr/dematerialisation_icp/dematerialisation_declar.htm

[85] Fédération informatique et libertés, "Cryptographie: un pas en avant, deux pas en arrière", 17 septembre 2002

[86] See also Certplus solutions for encrypted and certified email at http://www.certplus.com/cadres.htm?rub=offre$ssrub=certif_serveur$page=certif_serveur.htm

Encryption and anonymity

Encryption activists are perhaps more numerous in France because of the strict rules that have been an obstacle for more

Figure 3: September 2002 poll by FDI examining the reasons why 51 percent of those surveyed are not ready to use e-government services.

Prefer personal contact, face-to-face, with a representative of the administration	59 percent
Have no Internet access either at home or at work	40 percent
Have never used the Internet or do understand very well how it works	28 percent
Think the Internet is not yet a secure enough medium for completing administrative tasks	11 percent
Know of very few or no administrative services that can be accessed via the Internet	6 percent
Think that it's still to complicated to to perform administrative transactions on-line	6 percent

than a decade.

One notable development was announced by the French chapter of the Free Software Foundation in September 2002. The GNU activists succeeded in obtaining an authorisation from the Direction centrale de la sécurité des systèmes d'information (DCSSI), a Prime Minister's service, to distribute all releases of GNU-PGP. This is the open-source and general public licensed version of PGP, that implements strong encryption. When using key sizes longer than 128-bit key length, it needs special authorisation for providers, and a declaration for users. The problem is that every "user" of GNU-PGP is also a "would-be provider", because the source code is free and can be copied by anyone. The DCSSI, under the law, could have asked for special authorisation for every release made in France of GNU-PG. The DCSSI instead gave a single authorisation for the software. [87]

Another citizen-backed project that emerged in 2001 was the Renseignementsgeneraux.net. It mimics the "secret police" name (les Renseignemets généraux or RG) to give access to on-line forms in order to let citizens exercise their access rights to data files. Each request is then sent to the CNIL.

Finally, No-log.net was launched by the Internet provider Globenet. This service includes a procedure to limit the scope of data retention. All logs are encrypted, and the private key is shared among three of Globenet's executives.

[87] Communiqué de presse de la FSFE-France (Free Software Foundation Europe)

V. Other issues

Smart card systems

The Groupement d'intéret économique Cartes Bancaires (Gie-CB) is a private consortium of nearly all commercial and public sector banks. For over twenty years Credit cards in France have used a chip inside that requires a PIN code.

The Gie-CB tried to use the same system on the Internet (Cybercomm project), but it was a commercial failure. It was intended to be used with a portable smartcard reader that needed to be connected to the PC. But the hardware system was to be paid for by consumers; who were not interested.

The security of the French "carte bancaire" has always been criticized and tested by experts and hackers to find weaknesses; to little avail. The sole exception was in 1999, when an independent computer expert (Serge Humpich) proved it was possible to create "yes cards" by cloning a smart card that worked with any 4-digit PIN code. The GIE sued Humpich for revealing these "secrets". The tribunal's verdict was a deferred jail sentence of ten months.

The most recent banking gizmo in France is called "Moneo", and is like Proton in Belgium or Chipnik in the Netherlands. The consortium that provides it is called BMS and is backed by major GIE banks. It is an e-cash smartcard system that can be used for small purchases in newsprint outlets, restaurants, and bakeries. The consumers' organisation "UFC Que Choisir" condemned the system for being too costly for the consumer. More importantly, Moneo, at a bank's request, can record all transactions, point of sale and other details about a user. BMS, however, continues to say that the system is "anonymous".

Finally, transport utilities in Paris and Lyon have launched two smartcard systems. The Paris system (Navigo) is based on Calypso technology, and it could become an electronic wallet like Moneo. These transport passes - "contactless" smartcards – have a very high potential for invading privacy. All private data logs are recorded and retained, despite not having any legal requirement to do so; in Paris the data is retained for four years, while in Lyon it is retained for 13 months.

VI. Implications and conclusions

The issues of security and privacy could represent obstacles to the adoption of electronic services in France. As Pierre de La Coste argues:

> *"Certaines procédures administratives ne sont pas encore en ligne car elles nécessiteraient la mise en place de moyens de signature ou de cryptage. Aux notables exceptions près que constituent TéléIR et TéléTVA, les autres ministères ne disposent d'aucune téléprocédure grand public associant une signature électronique. ... il semble que les administrations autres que les Finances fassent preuve d'un attentisme qui pourrait conduire à un retard pour les téléprocédures ayant des besoins d'identification sécurisée, si aucune action rapide n'était engagée afin de lever l'attentisme actuel." 88*
>
> *[English: "Certain administration procedures are not on-line yet because they require the existence of the means for signatures or cryptography. With notable exceptions such as those created by TelelR and TeleTVA, no other ministries have available any public on-line procedure using digital signatures…it seems that government ministries other than the ministry of Economics and Finance are trying a wait-and-see policy, which could slow on-line procedures needing secure identification, if nothing is done to change this*

current attitude.]

[88] Ibid note 3.

Finally, public use, familiarity with e-government services and technologies are also inhibitors to its adoption. A number of surveys (see figures below) indicate that citizens prefer personal contact when interacting with government administration. Moreover, the public adoption of the Internet is still relatively low; even though they are aware of the availability of these services, and the security mechanisms involved. Citizens remain generally reluctant.

Privacy Enhancing Technologies and the United Kingdom [89]

I. Introduction

The United Kingdom is unusual in that it does not have a written constitution. The fact that the country is therefore essentially governed by "judge-made law" (in essence a "gentleman's agreement") is a fundamental aspect of its national character, with, arguably, two consequences. One: it implies a high level of trust in government by the public. Two: the absence of a written constitution makes it easy for those who determine public policy to feel that they are an elite who can settle things among themselves with little public scrutiny. The structure of the British Parliamentary system means that the party that has a majority in Parliament may pass legislation even against apparently widespread public opposition or indeed against the principles of law.

The Civil Service plays a vital, though often unrecognised, role in British government. It has been calculated that the average government minister stays in a given department approximately 11 months. The Civil Service, by contrast, tends to stay in placepermanently. The upshot is that the same legislative proposals may surface even after a change of government. A case in point is the provisions for government access to encryption keys. Originally proposed while John Major (Conservative) was Prime Minister, these proposals changed little after Tony Blair (Labour) came to power. The identity card proposal of the 1996 Conservative adminstration were re-introduced under the 2002 Labour administration with only cosmetic changes.

In addition, for historical reasons many people in the UK do not regard themselves as genuinely European, despite the country's membership of the EU. This attitude tends to reinforce result British arrangements in certain areas of security and communications that tends to mirror the desires of US law enforcement in these arenas .

In the areas of data protection and privacy, however, the UK is required by EU arrangements to pass national legislation supporting EU directives. In 1998 Parliament approved the Human Rights Act intended to incorporate the European Convention on Human Rights into domestic law. It was only then that an enforceable right of privacy was established in British law.

Protecting privacy is the responsibility of the Office of the Information Commissioner, formerly known as the Data Protection Registrar. This is an independent agency that maintains the register and enforces the Act. The Commissioner is also responsible for enforcing the Telecommunications (Data Protection and Privacy) Regulations.

The landscape for privacy in the United Kingdom is therefore confused. At some level, the public strongly recognises and defends privacy. On the other hand, crime and public order laws passed in recent years have placed substantial limitations on numerous rights, including freedom of assembly, privacy, freedom of movement, the right of silence, and freedom of speech. Closed-circuit television cameras permeate British society. Their original purpose was crime prevention and detection, but in recent years the cameras have become important tools for city center management and the control of "anti-social behavior". There are now well over one million such cameras covering public spaces. It is estimated that the average Londoner is caught on camera 300 times a day. Legal provisions for the limitation of rights of defendents, the establishmen of compulsory DNA testing, data retention, audit requirements and data matching have become core elements of public policy.

[89] Ian Brown, Simon Davies, and Wendy Grossman.

II. Legal landscape

Parliament approved the Data Protection Act in 1984 and updated it in 1998. The most recent legislation, which came into force on March 1, 2000, brings British law into accordance with the requirements of the European Union's Data Protection Directive. This legislation regulates the activities of both government and private entities, and is enforced by the Information Commissioner.

Nonetheless, the United Kingdom has set many standards for invading privacy. Legislation of this type is usually sponsored by the Home Office, which is charged with overseeing national security and law enforcement as well as immigration policy. Some initiatives, such as the Electronic Communications Act (2000), which contains provisions to register providers of cyprotgraphic services and also legalising digital signatures, arose from the Department of Trade and Industry.

The Regulation of Investigatory Powers Act (RIPA) became law in July 2000, superseding the Interception of Communications Act of 1985. It authorises the Home Secretary (the minister who heads the Home Office) to issue warrants for the interception of communications. It also requires Communications Service Providers to provide a "reasonable interception capability" in their networks. This requirement applies to telephone companies, mobile network operators, and ISPs, but is not necessarily limited to them. In June 2002 the government issued a list of some 200 authorities that it proposed to authorise to disclose access to data under RIPA. These included local authorities and quasi autonomous government organisations down to parish coun-

cil level, many government departments and even the Information Commissioner, all of whom would have been able to examine lists of websites visited, telephone and email contacts, and mobile phone location logs without a warrant. An outcry over the number of agencies caused the government to withdraw the list for reconsideration. Finally, RIPA permits senior members of the civilian and military police, HM Customs and Excise, and members of the judiciary to demand that users hand over the plaintext of encrypted material, or in certain circumstances the decryption keys themselves. Refusal carries a jail sentence of two years.

Other legislated practices are equally problematic. While police may demand identification before arrest only in limited circumstances, they now have the right to stop and search any person on the street on grounds of suspicion. Following arrest, a sample may be taken for inclusion in the national DNA database. The Crime and Disorder Act of 1998 provides for information sharing and data matching among public bodies in order to reduce crime and disorder.

The September 11, 2001 attacks in the US accelerated the UK's efforts in the direction of increased surveillance and decreased personal privacy. Legislative initiatives include the Anti-Terrorism, Crime, and Security Act (2001), and the Criminal and Justice Police Act (2001). The latter includes revisions to the Police and Criminal Evidence Act (1984) to bring law enforcement access to electronic communications into line with existing rights of access to more traditional communications.

In 2002, the UK government proposed rules under the Anti-Terrorism, Crime, and Security Act that would require ISPs to keep communications data such as logs of email correspondents, mobile phone location data, and Web site accesses for up to five years.

British privacy campaigners have anticipated that the European Parliament would provide some protection against too-invasive national laws. However, in 2002 the European Parliament, which until then had voted to ban the retention of communications data once it was no longer needed for billing purposes, changed direction and voted to allow data retention. Similarly, in February 2003 the European Commission provisionally agreed to allow British airlines to pass detailed customer data to American security services. There is a persuasive legal argument that doing so contravenes the European data protection laws, as the US does not have adequate legal protections in place to safeguard such data. But the US had threatened to ban flights from Britain if the data was not supplied.

III. Transformations in policy and technology

The general British public typically demonstrates only sporadic interest in information privacy. Even during the passage of the two controversial pieces of legislation that gave new surveillance powers to the government (the Regulation of Investigatory Powers Act 2000 and the Anti-Terrorism, Crime and Security Act 2001), public reaction was muted.

However, there have been notable exceptions. The negotiations over the exact provisions of RIPA in particular included an extended debate over cryptography policy, although this was largely limited to input by experts. The plan to allow 200-plus agencies access to communications data drew a very strong negative reaction from both media and public, forcing the Home Office to withdraw the plan for further consideration. Opposition to data retention has arisen from a number of sources, In early 2003, for example, an all-party Parliamentary working group issued a report condemning data retention and proposing instead data preservation. This last would entail a requirement for ISPs to keep data when a particular individual or organisation was under investigation, rather than retaining everything "just in case". The Home Office, however, continues to argue strongly in favour of data retention.

Most contentiously, in January 2003, the government ended six months of public consultation on proposals to introduce an "entitlement card" _ effectively, a national ID card _ to be backed by a centralised national database. The government seeks to persuade citizens to welcome this scheme by promising that it will cut benefit fraud, deter illegal immigrants from working, streamline government services, and prevent terrorism. In mid-January, the government claimed that the responses it had received to the consultation document had been overwhelmingly positive. A telephone response portal and Web site set up by Privacy International and Stand UK, however, collected more than five times as many responses in ten days, almost all of which were negative.

None of this has yet translated into a general public interest in technology that could ameliorate the impact of such legislation. Only one national ISP provides encryption software integrated into its default email client. No commercial Web or email anonymisation services have been created.

Because of the way the ISP market has developed, many providers even configure their networks in ways that reduce user privacy. Competitive pressures have forced ISPs to provide relatively cheap flat-rate Internet access packages. To reduce upstream bandwidth costs, many ISPs therefore force the use of Web caches that of necessity log the sites users have visited. In addition, to restrict the amount of junk email sent from their networks, some ISPs block connections

to other providers' outgoing mail servers, forcing all outbound messages to travel through their own mail servers — often logging details of all sent and received messages in the process.

Local government has shown scant interest in even the most basic privacy enhancing technology. Closed Circuit Television cameras are ubiquitous in many towns and cities, and footage has been passed on to third parties without the consent of those pictured or even an attempt to mask their faces [90]. The London Borough of Newham uses face recognition software on local CCTV images. A London-wide "Congestion Charge" scheme that recognises car number plates filmed by cameras is also to be used to attempt to track criminals [91]. In the process of setting up this scheme there was no public discussion of more privacy-friendly charging mechanisms such as anonymous pre-paid tolls.

London Underground is also introducing smart payment cards for use on buses and trains [92]. These devices will eventually also be capable of purchasing many other goods from shops in and around the transport network that are equipped with card readers. There has been little public discussion of the fact that the cards do not use any privacy enhancing technology such as allowing pre-payment with anonymous cash. All transactions and trips made using one of these cards are linkable and personally identifiable

In the summer of 2002 Privacy International discovered that over 1,000 schools around the UK have installed fingerprint readers. They are being used to check the identity of children when they borrow books from libraries [93]. The vendor's customer services manager stated in an interview that, "You may ask, why stop with library systems, when schools have so many concerns with registration, attendance, and security? I assure you, we are way ahead of you. Watch this space..." [94]

Surprisingly, the fingerprinting system was welcomed by the Office of the Information Commissioner, which assured the vendor that its system "aids compliance with the Data Protection Act." [95]

[90] Clare Dyer, "Suicide bid on CCTV may herald new privacy law", The Guardian, 29/1/03.
http://www.guardian.co.uk/uk_news/story/0,3604,884193,00.html

[91] Mark Townsend and Paul Harris, "Security role for traffic cameras", The Observer, 9/2/03.
http://www.observer.co.uk/waronterrorism/story/0,1373,892081,00.html

[92] http://www.londontransport.co.uk/tfl/prestige_project.shtml

[93] http://www.privacyinternational.org/countries/uk/kidsprint/

[94] http://www.microlib.co.uk/images/events/revp2.jpg

[95] http://cgi.www.microlib.co.uk/cgi-bin/www.microlib.co.uk/default.asp?action=page&page=/news/articles/A3/index

IV. PETs in the UK

A small number of UK and multinational companies have launched privacy-enhancing products. As can be seen from this short list, this seems to be a contracting rather than expanding market.

SafeDoor [96] was a pseudonymised shopping service provided by the multinational delivery service Securicor. Customers could register their name, address and credit card details with the company, and then make purchases at affiliated merchant sites using a username and password provided by SafeDoor.

Payment was made direct by SafeDoor to merchants for purchases made by its members, and then charged to members' credit cards. Goods were delivered directly by Securicor. Members therefore did not need provide any personally identifiable information to merchants. They also received increased protection against credit card fraud. The service was discontinued in May 2002. No other delivery company provides an equivalent service.

The ISP Demon Internet [97] provides all customers with an email client called Turnpike that contains built-in PGP encryption and authentication mechanisms. Turnpike can be set to automatically encrypt messages to all users who have made a public key available, and to automatically decrypt messages as they are received. Turnpike does not, however, protect message header information such as sender, recipient or subject.

The Internet Service Providers' Association has attempted to prevent the imposition of a data retention scheme since the passage of the Anti-Terrorism, Crime and Security Act 2001 gave the government the power to impose one. At present, ISPs store communications data (such as the details of who customers have sent and received email to and from and the websites they have visited) for a very short period of time (often just hours or days). The government has been drafting a "voluntary" code of practice that would extend retention to up to one year for this information. ISPs, based on a legal opinion obtained by the Information Commissioner, rejected this as a disproportionate invasion of their customers' privacy [98]. The Home Office almost alone believes that it can create a human rights-friendly data retention scheme, and continues to consult with industry on how to do this [99].

[96] http://www.safedoor.co.uk/

[97] http://www.demon.net/

[98] http://www.apig.org.uk/ispa.pdf

[99] http://www.apig.org.uk/homeoffice.pdf

IPv6

IPv6 has yet to become widespread in the UK. The only publicly-available trial service was run by NTT Europe from December 2000 to December 2002. The company is now preparing to launch a commercial service.

Research networks have also been running IPv6 on a trial basis for several years. The government-funded Bermuda 2 project is examining the issues involved in deploying IPv6 across the UK academic network, JANET. The major participants in the trial are the University of Southampton, the University of Lancaster, and University College London.

The UK IPv6 Task Force was formed in 2002 to encourage UK users to migrate to the new protocol. Its home page [100] contains links to the organisations and activities involved in this work, including all of those mentioned above.

[100] http://www.uk.ipv6tf.org/

PKI

Public-Key Infrastructure technology became controversial in the UK during the late 1990s as the government attempted to use it to impose mandatory key escrow. Planned legislation would have required organisations and individuals to deposit the private half of a key pair with any member of a network of "Trusted Third Parties" as a condition of certifying the public half of the key. The private key would then have been provided to law enforcement agencies when they wished to decrypt data that had been encrypted with the related public key. A particularly contentious provision of the law was a requirement that anyone issued with a decryption order keep it secret. People under investigation, therefore, whether or not they were eventually convicted or even charged, would face criminal charges if they notified their correspondents that their privacy in turn was also being breached.

Commercial organisations objected on the grounds of the security risks this would create. There were also privacy objections from the public and civil liberties organisations. These protests eventually paralysed the key escrow plan. Certification Authorities were left to develop according to market demand.

Demand for certificates has so far proven to be very limited. The **Royal Mail** launched a service called Viacode based on Entrust's PKI software in 1998. It issued digital certificates to a number of public and private sector organisations. However, it ceased trading in August 2002 because of an "unsustainable financial position caused by the slow development of the market and the limited take up of digital certificates." [101] The British Chambers of Commerce also for a time offered a certification service called Chambersign, which is still listed as an acceptable provider on the HM Customs and Excise Web site for accessing electronic services, but is no longer issuing new certificates.

The UK government is still attempting to promote the take-up of digital certificates. Agencies such as the Inland Revenue (tax authority) and HM Customers and Excise, among others, accept information authenticated using certificates rather than the less secure combination of username and password. However, the withdrawal of Viacode and Chambersign leaves Equifax and BT Trust Services as the only accepted providers of certificates for this service. [102]

[101] http://www.viacode.com/

[102] http://ggh.ukonline.gov.uk/GGH/GGHelp/0,2404,139261~522700~~en,00.html

Encryption

The Regulation of Investigatory Powers Act 2000 will give UK law enforcement agencies the power to demand decryption keys or that users decrypt specified encrypted data. A team of volunteers is developing m-o-o-t [103], a suite of software that will minimise the amount of information such powers can be used to access.

m-o-o-t will protect both communications and stored data. Links are encrypted using keys that are thrown away after each session ends, so that a user cannot be forced to decrypt captured ciphertext. Files are stored using multiple steganographic file systems. These allow different files to be protected by different passwords. A user may therefore reveal one password under legal duress that gives access to a set of unimportant files while concealing more sensitive information.

The key research into privacy-enhancing technology in the UK is being undertaken by Cambridge University's Security Group [104]. Ross Anderson has conducted extensive research on medical record pseudonymity and cipher design. Richard Clayton is looking at failures of anonymity systems and the traceability in general of Internet communications. George Danezis is developing anonymous and pseudonymous communications protocols, and has implemented Ron Rivest's Chaffinch system for providing confidentiality and plausible deniability using only authentication mechanisms. He is part of a design team creating a more advanced anonymous remailer called MixMinion. Andrei Serjantov is developing a theoretical anonymity framework and using it to measure the amount of anonymity that users of an anonymising network of mail mixers experience. The practical aim is to develop systems that can provide users with guarantees of

specific aspects of anonymity.

Royal Holloway College is also conducting several security projects [105], although with less of a privacy focus. They have recently taken part in projects to develop USB cryptographic tokens, privacy requirements for future mobile telephony equipment, and an evaluation of cryptographic algorithms for standardisation at a European level.

Smaller research groups are located at Oxford University [106] (developing analysis tools for security protocols and information flow), Salford University [107] (looking mainly at PKI), and the London School of Economics [108] (examining security issues from a social science perspective).

The government has funded some research on privacy enhancing technologies through its Research Councils. The Economic and Social Research Council, for example, funded a project on "Human Issues in Security and Privacy in E-commerce" that included an investigation into the "State of the Art in PETs" [109]. The Engineering and Physical Sciences Research Council also regularly funds research into security mechanisms, although rarely with specific application to privacy.

[103] http://www.m-o-o-t.org/

[104] http://www.cl.cam.ac.uk/Research/Security/

[105] http://www.isg.rhul.ac.uk/research/projects.shtml

[106] http://web.comlab.ox.ac.uk/oucl/research/areas/concurrency/research/security/

[107] http://sec.isi.salford.ac.uk/

[108] http://csrc.lse.ac.uk/

[109] http://www.hispec.org.uk/public_documents/PETReview3%207.1.doc

V. Other issues

Three key government reports have discussed issues relating to privacy enhancing technologies over the last few years. These provide the clearest indication of the direction the government will take in these matters.

The Privacy and Data-Sharing report [110] from the Performance and Innovation Unit (now merged into the Cabinet Office's Strategy Unit) was published in 2002. It looked at the issues raised by increased sharing of personal data within government. Such sharing has reached a high level on the political agenda, ostensibly in the interests of allowing more efficient and personalised services and encouraging what the Labour Party describes as "joined-up government". Essentially, this expression simply means sharing data across departments, which the government claims will make it possible to offer the public the kind of streamlined service people have come to expect (in theory at least) from the corporate sector.

This report acknowledged that it was vital to gain public trust in the security and privacy of their data to deliver these benefits. It suggested that government should follow the principle of "least intrusion" by requesting the minimum amount of personal data required to provide a service, and that citizens should have the maximum choice possible over the management and use of their data.

The report contained one section on security technologies that can enhance privacy. It described P3P, PKI, biometrics and smartcards, and their potential uses within government. The report recommended that government should continue to monitor new technology for its potential to protect privacy, and that it should set up a programme of demonstration pilots using smartcards. It also recommended that the ISO 17799 information security standard be applied across the public sector to protect personal information. Funding for these recommendations must be negotiated during the government's normal spending decision processes.

The Home Office launched a national consultation on the introduction of a national identity or "entitlement" card in 2002. This card would "provide people who are lawfully resident in the UK with a means of confirming their identity to a high degree of assurance; establish for official purposes a person's identity so that there existsone definitive record of an identity which all Government departments can use if they wish; help people gain entitlement to products and services provided by both the public and private sectors, particularly those who might find it difficult to so do at present" and "help public and private sector organisations to validate a person's identity, entitlement to products and services and eligibility to work in the UK."

The fact that there are only ten occurrences of the word "privacy" in the 147-page consultation document [111] indicates how little attention was paid to the issue and how much emphasis is placed on the concept of data protection. No specific section of the report examines privacy-enhancing technologies. Smartcards and biometrics are described, but mostly in relation to their ability to reduce fraud.

The National Health Service set up the Caldicott Committee to investigate flows of patient-identifiable information not related to direct care or medical research. The committee published its "Report on the review of patient-identifiable information" in December 1997 . Two of its 16 recommendations encourage the use of privacy enhancing technologies: "Where particularly sensitive information is to be transferred, the use of privacy enhancing technologies (e.g. encrypting the NHS number) must be urgently explored" (recommendation 10) and "institutions providing training in healthcare informatics are encouraged to include privacy enhancing technologies as part of those training pro-

grammes" (recommendation 11). So far, however, little has been done to implement these recommendations, even in simple cases such as the Clearing payment system, where patient name and address is included in the treatment records used to make payments to healthcare providers [113]. An NHS consultation on confidentiality ended in February 2003; it remains to be seen whether its output will have more impact than the Caldicott report.

[110] http://www.strategy.gov.uk/2002/privacy/report/

[111] http://www.homeoffice.gov.uk/cpd/entitlement_cards/cards.htm

[112] http://www.doh.gov.uk/confiden/crep.htm

[113] http://www.fipr.org/press/030205NHS.html

VI. Implications and conclusions

The situation in the United Kingdom is quite mixed. Privacy is a component of many of the public discourses in the media, although successive governments have failed to appropriately and adequately address privacy concerns. The development of PETs is limited, and generally unsupported by policy directions from the government.

There is some hope, however. Trust is a concern of both industry and government, and this may be supported through an appropriate authentication system. While Royal Mail has abandoned the Viacode solution for PKI, other infrastructures may be developed and there remain opportunities to embed privacy-enhanced authentication systems in its stead. We have received indications from the Cabinet Office division responsible for all electronic affairs, the 'e-envoy' that they have looked favourably upon such privacy enhanced developments. Such a system may support trust

There is some recognition generally that PETs and public policy are a good mix for generating trust. The joined-up government proposal discussed the potential for PETs (although using outdated understandings of the technology available at the time), understanding that trust could be developed in the scheme with the use of technology. One would hope that this would generate sufficient interest in industry to develop appropriate solutions.

Technology may provide the link in the UK between what the citizenry is seeking and what the government may be willing to provide. The response to e-government has been relatively poor, as findings have indicated recently. [114] It is our hope that this may lead the government to consider trust and privacy issues more seriously.

As it is, the situation is bleak. In a poll from September 2002, the majority of British voters claimed that they do not trust the government with the details of their private lives: 58% disagreed with the statement that the government can be trusted to keep their personal data secure. [115]

The government is not unaware. A copy of the minutes of the government's high-level "Senior Group on Information Policy" "leaked" last year to the BBC's "Today" programme indicated a high level of sensitivity about the current low level of public trust, together with concern over a "general public antipathy" about the prospect of data sharing. Ironically, when the BBC requested those minutes under the Open Government process, nearly all references to trust had been removed, as had all references to the Cabinet Office requiring departments to provide information on subject access requests under the Data Protection Act submitted by Opposition MPs. [116] Apparently, a change in practices is not imminent.

[114] UK 'lags in e-government', BBC-Online. http://news.bbc.co.uk/1/hi/technology/2794095.stm

[115] Privacy fears revealed, The Guardian, available at http://www.guardian.co.uk/bigbrother/privacy/statesurveillance/story/0,12382,787808,00.html

[116] source: Senior Group on Information Policy. Minutes of the meeting of 12th September 2002, London.

Section III. Technology and Privacy Developments in Europe

In order to support policy-making, the European Commission has created the "European Research Area" (ERA) to implement European research programmes in legal and political obligations resulting from the treaties of the EU. This research mandate is therefore supported by the treaties of the EU, particularly the Amsterdam Treaty. In the Amsterdam treaty an entirey chapter discusses the essential role played by research and technological development to the functioning of industralised countries.

To support the ERA, the European Commission, Member States, and the European Parliament developed a series of initiatives, including the 'framework programmes for Research and Technological Development' (FP). The 5th such framework (FP5) spanned the years of 1998-2002, while the 6th framework (FP6) is from 2002-2006. The budget for FP6 is 17.5 billion euros, an increase of 17% over FP5; and represents 3.4% of the EU's total budget in 2002.

A number of 'key areas' or 'thematic priorities' are earmarked to achieve the objectives of each framework. Both FP5 and FP6 include the key area of 'information society technologies' (IST), and within the IST area, a number of research projects involve privacy and technology. These projects, sometimes to develop 'roadmaps' for further work, other times to develop demonstrations and proofs of concept, are often conducted by 'consortia'. The consortia tend to involve the co-operation of a number of sectors of society, including NGOs, industry organisations (even cross-sector, and varying in size from multinationals to small and medium sized enterprises (SMEs)), universities, research institutions and other centres of 'expertise' and 'excellence'.

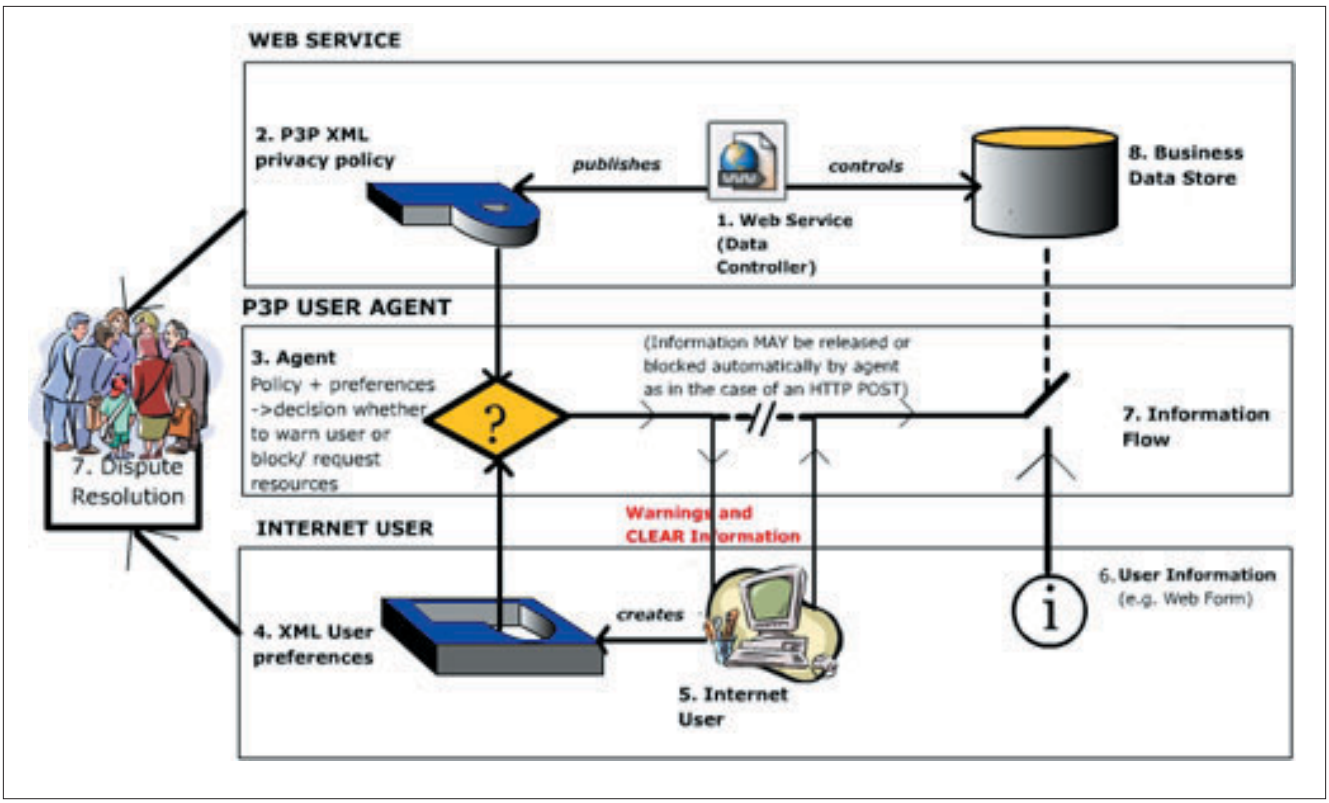
In this section we will review some of the research projects in progress, most notably the user-level Platform for Privacy Preferences (P3P), best practice guidelines for adherence to the EU directives (GUIDES), Privacy Enhancement in Data Management in E-Health (PRIDEH), and Privacy Incorporated Software Agent (PISA). The second generation research on privacy and technology involves two 'Roadmap' projects, with one project on privacy and mobile communications (PAMPAS) and another privacy and identity management (RAPID).

P3P

Posting a privacy policy on a Web site is not sufficient to put a Web site into compliance with the requirements arising from articles 10 and 11 of DPD 95/46/EC. Once a privacy policy has been posted, it may form the basis for legal liability.

P3P offers a technical solution to the problem of managing the privacy preferences for on-line users. Privacy practices are 'translated' into a standardised, machine-readable format (Extensible Markup Language XML). According to the JRC, the flow is as follows [117]:

[117]:Taken from http://p3p.jrc.it/aboutP3P.php



Users decide the threshold of information disclosure they find acceptable, and P3P installed in their browser negotiates with the server's 'translated' privacy policy. According to the W3C [118]

> *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. In short, the P3P specification brings ease and regularity to Web users wishing to decide whether and under what circumstances to disclose personal information. User confidence in online transactions increases as they are presented with meaningful information and choices about Web site privacy practices.*

[118] Taken from http://www.w3.org/P3P/brochure.html

The effectiveness of P3P is controversial however. The W3C admits that "P3P does not set minimum standards for privacy, nor can it monitor whether sites adhere to their own stated procedures."

The EU Data Protection Working Party, along with EU-funded research, stress that P3P does not guarantee compliance to data protection legislation. It does, however, provide an extra level of support for the issue of transparency, and does so in a way that can be integrated seamlessly into the user's browsing environment, and which can prevent end users from having to read through lengthy and complex online privacy statements to ascertain whether they trust the data processing policies of a site sufficiently to enter into business transactions using it. [119]

[119] JRC and PWC. GUIDES: Final Guidelines Document. Brussels: European Commission, April 8 2002, p.42. Available at http://eprivacyforum.jrc.it/default/page.gx?_app.page=entity.html&_app.action=entity&_entity.object=KM------00000000000002C8&_entity.name=guidelines.pdf

The Joint Research Centre, a Directorate-General of the European Commission that provides independent scientific and technological support for EU policy-making, runs a project on P3P that develops a demonstrator. This project has a number of aims, among which are

1. *Provide Consumer Education: The P3P demonstrator will provide the EU with a commercially independent implementation of the standard within an interactive tutorial environment.*
2. *Increase Consumer Confidence: The demonstrator will contribute to the theme on promoting the European development of e-commerce by increasing consumer trust and confidence in on-line electronic transactions.*
3. *Understand End-User Reactions: The demonstrator will be used to gauge the success of the standard, in its initial implementation, from the subjective perspective of end users.*
4. *Platform for extended research: The implementation will serve as a research platform for experimental extensions on the P3P standard. In particular, the implementation should provide an architecture, which facilitates a secure and efficient basis for the investigation and possible implementation of extensions to strengthen the privacy protection.*
5. *Integrated Research Platform: The implementation will permit the JRC to assess the standard from the perspective of its integration into trusted on-line systems which deploy emerging security management technologies and other Privacy Enhancing Technologies (PETs) (for example, cookie crushers and anonymiser technologies).*
6. *Privacy Compliance Platform: Increasing the effectiveness with regards to data protection compliance. That is, many have argued that the EU legislation makes personal data protection a legal requisite, not an issue for negotiation between a business and a consumer. P3P supports the latter. The implementation will allow these questions to be explored in greater detail, and will support ongoing JRC activities addressing the development of Privacy Compliance Guidelines for the Commerce Sector.* [120]

Efforts to strengthen the protocol include the introduction of a semantics architecture, the developmnet of a proxy service, and the use of the SOAP protocol to create a distributed version of P3P.

The guidelines mentioned in item 6 of the P3P project are discussed in further detail in the next section on research at the Commission. Meanwhile, the W3C is planning its own set of innovations regarding P3P, particularly involving PURPOSE elements to describe the primary purpose of data collection; adherence and compliance with the EU Directive, e.g. example, an element to explain what jurisdiction data is going to, and another element to describe maximum data retention period. [121] These will be further developed in a June 2003 meeting in Kiel, Germany.

[120] Adapted from http://p3p.jrc.it/aboutthisproject.php

[121] Cranor, L., and Weitzner, D. Summary Report — W3C Workshop on the Future of P3P. Dulles, Virginia: W3C: Technology and Society Domain,

November 12-13 2002. Available at http://www.w3.org/2002/12/18-p3p-workshop-report.html

GUIDES: E-Business Guidelines on DPD 95/46/EC

The primary goal of the GUIDES project was to develop a set of best practice guidelines to assist European e-business adherence to the EU data protection regime. That is, the guidelines are a mix of legal and technological guidelines, clustered around privacy principles supported by the EU directives. It is concerned particularly with the technology-related privacy challenges raised by the HTTP protocol (including additional disclosure of information such as web browser, Operating System, and advances such as IPv6 that may be more static and disclose geographic location), web bugs and cookies, e-profiling.

In the conduct of e-commerce, GUIDES notes that

- The interdependencies between on-line companies are growing and data flow between them is increasing, placing a greater strain on the privacy of Personal Data.
- Although privacy policies and seals from trustmark organisations are more and more common, the "trust-value" of these seals are not always clear
- P3P is emerging as an important technology standard for managing consumer privacy preferences in the on-line domain;
- Multinationals are most likely to have resources to implement privacy policies and procedures; Small and Medium-sized enterprises typically do not have these resources. [122]

[122] JRC and PWC. *Final Report — GUIDES Deliverable D5.2.* Brussels: European Commission, April 2002, p.5. http://eprivacyforum.jrc.it/default/page.gx?_app.page=entity.html&_app.action=entity&_entity.object=KM------00000000000002C8&_entity.name=final.pdf

Similarly, for mobile commerce, the project concludes that

- M-commerce regulation and standards have difficulty to keep up the pace.
- Some e-commerce PETs are transformed into m-commerce PETs (mobile P3P, WTLS)
- M-commerce privacy risks are more complex than e-commerce privacy risks
- M-commerce business models are WAP focused and transactions are low in volume and expensive. As soon as GPRS/UMTS/CDMA takes off and transactions are high in volume privacy will become more and more important. [123]

[123] ibid.

As a result of these concerns, the guidelines describe 'best practice' for adhering to the EU Directive 1995. Many of the proffered solutions are not technological in nature, and are rather policy-level. There are some technological recommendations, however.

Particularly for the security principle of data protection, the GUIDES project recommends that

- An e-businesses should ensure that that all security-related vendor software patches are promptly installed and that questionable software is not installed;
- An e-business should configure its e-commerce systems to listen for Internet packets only on those ports assigned to applications that are actively used on the e-commerce system;
- An e-business should only use downloaded software from a 'trusted' source;
- The system administrators of an e-business should tightly control physical access to e-commerce system hardware. Only authorised members of the technical staff should be allowed access to systems;
- An e-business may implement audit procedures (e.g., tracking who is accessing the data, what data was accessed) combined with analysis of audit logs and follow-up for unauthorised or anomalous activity is essential for long-term system security and privacy.
- An e-business may use secure database products to ensure the safety of data. Multi-level secure databases segregate data into areas where users may or may not have access (limiting data access via database engine passwords or digital certificates separate from the operating system password adds another layer of security);
- Identifying users before they access the e-business network is a key component in protecting information resources. (...) Password procedures and an authentication system with encrypted password protocols will help the e-business close the loopholes that intruders use to compromise systems.
- Passwords; the basic function of a password typed in at a remote terminal or web browser is to prove to a central server that the user really is who they say they are.
- Implement effective physical, technical, and procedural measures to secure personal information on a Web site and linked computer systems.
- The e-business should establish appropriate access and verification procedures, audit trails and record integrity controls. [124]

[124] JRC and PWC. GUIDES: Final Guidelines Document. Brussels: European Commission, April 8 2002, p.31.

These security procedures are expected to be met using network-layer security mechanisms. E-businesses, according to GUIDES, should

- *deploy routers that selectively block packets when routing them from one network to the other. A screening router uses a set of pre established rules that define the packets that may be passed (packet filtering);*
- *implement firewalls between its internal network and the public Internet. (...)*
- *deploy intrusion detection systems to monitor usage of information systems and data in near-real-time and to block patterns of behaviour that appear to violate system security or privacy policies;*
- *use proxy-servers,*
- *tightly control physical access to network hardware. Only authorised members of the technical staff should be allowed access to hardware;*
- *investigate breaches of security should be investigated properly and remedied, particularly when damage or distress could be caused to an individual, an e-business should use e-commerce systems that keep audit trails for the detection and dealing with breaches of security;*
- *use fibre optic network cabling is preferred over copper wiring for systems requiring high levels of protection as these are less easily intercepted than over other copper-based alternatives.* [125]
- *At the application-layer, mechanisms are also advised. E-businesses should*
- *use SSL (secure sockets layer) to protect server-client communication with server authentication, confidentiality and integrity services.*
- *use electronic payment systems that are authenticated, resistant to forging and confidential;*
- *use WTLS (wireless transport layer security) for m-commerce applications which provides the same functionality as SSL;*
- *consider deploying authentication systems for downloading software. Signed downloaded objects ensure that software has not been tampered with;*
- *also deploy client digital signature services to achieve e.g. non-repudiation;*
- *use secure messaging or S/MIME to ensure the security needs of messaging applications.* [126]

[125] ibid, p.35

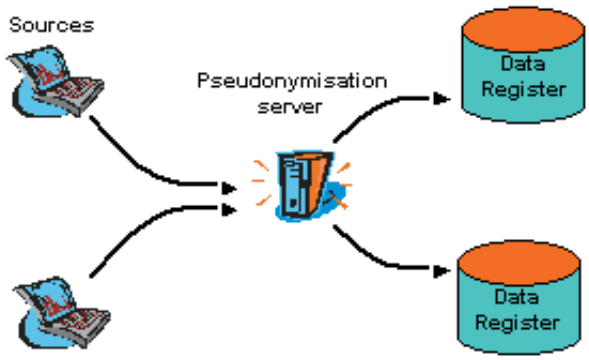
[126] ibid, p.33

PRIDEH: Privacy Enhancement in Data Management in E-Health

PRIDEH researches and promotes the adoption of privacy enhancing technologies in healthcare, and later in other areas. The project consists of three members: CUSTODIX, a Belgian-based trust service provider of pseudonymisation and other security services; WREN Computing a developer of security functionality in its application software; and Ernst & Young Audit (France) involved in security auditing of various applications.

The project's main concern is that identities are usually used as 'keys' for managing information, which leads to privacy problems. Rather, PRIDEH promotes, though technology, a provision of a 'secure' means of handling data that attempts to minimise the risk of privacy infringement while still taking advantage of the benefits from clustering and following up information coming from various sources and collected over time through pseudonymisation services.

The pseudonymisation involves the use of a Trusted Third Party (TTP) scheme.



Their argument is that secure and acceptable ways of working must rely on a trusted service provider for privacy enhancing techniques, i.e. pseudonymisation services. This entity guarantees a secure operation and safeguards all keys and methods in the process. The project is due to be completed in the fall of 2003. [127]

[127] See http://www.prideh.custodix.com/ for more information.

PISA: Privacy Incorporated Software Agent

The goal of this project was to develop an electronic intermediary to protect the user's privacy. This involved a filter called the Identity Protector (IP) to remove all unnecessary linkages to a user's personally identifying information. The aims, as originally articulated were

> *Demonstrating Privacy Enhancing Technology as a secure technical solution to protect 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. [128]

[128] From http://www.singleimage.co.uk/pisa.htm

That is, rather than relying on legal protection and self-regulation only, the project leaders believed that protection of consumers' privacy is probably more effective if transactions are performed by means of technologies that are privacy enhancing.

The PISA consortium is intended as a proof of concept, to demonstrate that it was possible to perform complicated actions on behalf of a person, while protecting that individual's personal data from compromised. The PISA demonstration model would incorporate a number of technologies

- *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.*

The demonstration involved applying the solution in two cases, one involving searches on job sites, and the other involving purchases of vehicles and real estate.

This work, to the knowledge of the authors of this report however, remains incomplete.

Mobile Privacy and Privacy and Identity Management

With another round of funding under FP5, the European Commission DG Information Society launched 25 'Roadmap' projects in 2002. [129] Two of these Roadmap projects were Pioneering Advanced Mobile Privacy and Security (PAMPAS) and the Roadmap for Advanced Research in Privacy and Identity Management (RAPID).

[129] Information Society Technologies. Roadmap Projects in IST Key Action II — New Methods of Work and Electronic Commerce. Brussels: European Commission DG Information Society, August 21 2002. Available at http://www.ercim.org/reset/Roadmaps_list.pdf

PAMPAS

Launched in June 2002, PAMPAS aimed to identify issues in mobile privacy and security with the goal of producing a framework for further research to be proposed under the 6th Framework (FP6), for 2003. PAMPAS aims to ensure that mobile services and systems satisfy security, privacy, and identity management requirements.

The project, lead by Ericsson Eurolab, identified a number of facets to privacy and identity management that require further research. These include

- *Privacy-preserving mobile applications with tuneable anonymity, calling for research and evaluation of application-specific privacy-preserving solutions. This involves creating a model for measuring the degree of anonymity that should be provided based on the service and application. "This would help finding the balance between on the one hand privacy and personalisation (e.g., the banner application), and on the other hand privacy and performance (i.e., most current solutions for anonymous communication trade off anonymity with bandwidth efficiency)."*
- *Models for anonymity and pseudonymity would involve the implementing of network protocols to provide for varying levels of protection, e.g. Crowds and Onion Routing protocols.*
- *Authorisation privacy, particularly as "too often a lot of personal information is distributed to enable access control".*
- *User-centric mechanisms allowing controlled release of personal information*
- *Deployment of Internet anonymisation tools for mobile networks*
- *Evolution to anonymising peer-to-peer networks*
- *Single Sign-On based on mobile authentication, in opposition to the Microsoft Passport and Liberty Alliance authentication mechanism. PAMPAS proposes that mobile operators could play an important role in developing their own model of authentication.*
- *Location based services versus location privacy*
- *Scaleable Privacy Preservation, involving research and evaluation of solutions for preserving the mobile users privacy to balance privacy and personalisation, "where the degree of anonymity is managed by and for the mobile user in a trustworthy and feasible manner."* [130]

[130] Listed adapted from PAMPAS. *Refined Roadmap for Pioneering Advanced Mobile Privacy and Security*. Pioneering Advanced Mobile Privacy and Security, February 28 2003.

among many other initiatives for further research. The intention is to take this forward under the new funding framework.

One company doing work related to the PAMPAS project, Open Business Innovation from Denmark, is work-

ing on developing authentication mechanisms for wireless applications that is privacy enhancing. They argue for an approach that combines an offline privacy enhancing accountability process (escrowed identity disclosure process) with a privacy-managed Public Key Infrastructure providing pseudonym support. This is applied particularly for location and privacy enhanced wireless client devices through which the end user will control multiple non-linkable, but accountable identities. Such a system is ideally suited for e-government and especially multi-hub healthcare. By moving straight to privacy enhanced multi-identity e-government, Open Business Innovation argues that the core problem of national identification systems may be resolved.

RAPID

Another Roadmap project, RAPID, is a collection of experts from industry, academia and research institutions, and civil liberties organisations that cover the domains of privacy enhancing technologies, IT security , law and IT and socio-economic issues. The goal was to discover and construct the technological, legal and methodological basis for solutions for a privacy-protected world. The longer-term goal was to facilitate the roll-out of live systems offering real protection to citizens' privacy, while respecting other constraints such as usability and security. [131]

[131] http://www.rapid.org/default/page.gx?_app.page=entity.html&_app.action=entity&_entity.object=KM------00000000000003FE&_entity.name=PETfactsheet

The core concept to RAPID was 'Privacy Enhancing Identity Management (PIM)'. PIM offers a means whereby individuals control the nature and amount of personal information about them that is disclosed. This concept was to be applied to privacy enhancing technologies in infrastructures and enterprises. The latter research was led by PriceWaterhouseCoopers, IBM, HP, Siemens, and Ericsson.

The requirements behind PIM, as identified by RAPID, are based on

- EU data protection directives;
- User preferences and enterprise privacy policies;
- Common Criteria requirements [ISO/IEC IS-15408] with the following properties:
  >> Anonymity ensures that a subject may use a resource or service without disclosing the user's identity.
  >> Pseudonymity ensures that a user may use a resource or service without disclosing its identity, but can still be accountable for that use.
  >> Unlinkability ensures that a user may make multiple uses of resources or services without others being able to link these uses together.
  >> Unobservability ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.

and they believe that PIM will lead to a reduction of costs (particularly adherence to data protection regulations within the enterprise environment), integrated compliance, improved security, and possibilities for new services delivery, such as single-sign-on portals.

One of the primary envisioned areas for application of PIM by RAPID is within e-government delivery. Data integration projects are centralising and interconnecting data sources; but in many cases, RAPID argues, data integration happens without specific purpose definition. Rather, this integration appears to be driven by the mere fact that it is feasible to interconnect data. Obviously problematic from the privacy and data protection perspective, RAPID argues that e-government development in EU countries requires an efficient identity infrastructure for the various (offline and on-line) information relationships between government and citizen. Of course natural suggestions of PKI and e-identity cards may arise, but RAPID believes that we must develop systems that allow for a range of anonymity or pseudonymity within this identity infrastructure; and even 'partial identities', which are a subset of properties regarding an individual, and multiple identities. [132]

[132] Samarati, P., Damiani, E., and Vimercati, S. D. C. d. Identity management PIM Roadmap: 'Multiple and Dependable Identity Management: R & D Issues'. Roadmap for Advanced Research in Privacy and Identity Management, December 20 2002. Available at http://www.rapid.org/default/page.gx?_app.page=entity.html&_app.action=entity&_entity.object=KM------000000000000042B&_entity.name=draft-identity-management

That is, a successful identity management system for any application area, according to RAPID, should support

- Reliability and dependability. While their main goal is to protect and preserve individual users' anonymity, digital identities should fully guarantee other parties that the identity can be relied upon, and therefore obligations to the digital identity deriving from such a transaction will eventually be met by someone.
- Controlled information disclosure. Users must be given control on what identity to use in specific circumstances.

The minimal disclosure of credentials appears to be the ideal way forward. A 'credential', according to RAPID, is any information about the user asserted either by the user herself/himself or by another party or process. [133] Traditional credentials are ill-suited for such applications, however, as they always provide the same amount of information when disclosed regardless of the specific transaction. More modern privacy-friendly credentials are required, as they reveal only the information strictly necessary to perform a transaction.

Without the necessary technology, the RAPID project participants believe that compliance to privacy regulations is meaningless. That is,

> *The trend is to state and adhere to policies compliant with appropriate legislations and regulations. Definition of compliance in terms of an externally stated privacy policy has limited meaning as externalised policies (e.g., using P3P) are quite coarse-grained and allow many interpretations (depending on assignment of specific organization-internal entities and processes to external role and purpose variables). Also, even a fine-grained external policy is only meaningful if organizations can match their complex business processes against their stated policies; and policy enforcement can be automated and verified. In addition, a fine-grained and enforced policy may be compliant with legislation and requirements for data minimisation; however, the extent to which governments and users can require and verify data minimisation depends to a large extent on the use and awareness of emerging privacy-enhancing technologies. Therefore, without a definition of compliance, without appropriate awareness and advances in technology, and without means to enforce policies, 'compliance' has limited meaning.* [134]

[133] Ibid.

[134] Herreweghen, E. v., Waidner, M., Bramhall, P., Cuellar, J., Tappe, J., Holtmanns, S., and Schasfoort, F. Enterprise PIM Roadmap: 'Privacy Enhancing Technologies and Identity Management Systems in Enterprises'. Roadmap for Advanced Research in Privacy and Identity Management, November 17 2002. Available at http://www.rapid.org/default/page.gx?_app.page=entity.html&_app.action=entity&_entity.object=KM------0000000000000432&_entity.name=draft-enterprise

The Roadmap is near completion as the groups involved in RAPID are working on getting FP6 funding under a new project title Privacy and Identity Management for Europe (PRIME). Organisations involved include IBM-France, IBM-Research Zurich, PriceWaterhouseCoopers, Dresden, HP and a number of European universities. PRIME is a four-year project that intends to develop solutions to empower individuals to control their private sphere and manage their identities, and to trigger pervasive deployment of privacy-enhanced identity management solutions.

We can already predict some of the technologies that may emerge from this further research, however; particularly as some work has been conducted in the private sphere specifically on developing such solutions.

For example, Hewlett-Packard, mostly from its labs in Bristol, has been researching Identity Management systems. HP's researchers accept that more sophisticated means of identity management than mere PKI are required, particularly a system that allows entities to identify themselves in such a way that fosters trust and respect for privacy and data protection. Even more modern solutions are inadequate.

> *The current trend towards federation of identities for distributed services, both on the Internet and across enterprises and organisations, on one hand provides new business opportunities to users and service providers but on the other hand it introduces new threats. Single-sign-on components, including those proposed by Microsoft .MyServices and Liberty Alliance Project, allow entities to authenticate once and access services supplied by multiple providers. Hackers or third parties can take advantage and misuse this process. (...) They need to be secure and compliant with privacy laws and data protection legislation.* [135]

[135] Mont, M. C., Bramhall, P., Gittler, M., Pato, J., and Rees, O. *Identity Management: a Key e-Business Enabler.* Bristol: Hewlet Packard Laboratories, June 12 2002. Available at http://www.hpl.hp.com/techreports/2002/HPL-2002-164.pdf

HP predicts that multiple 'views' of identity are going to be available, some of them directly under control of the owner, others managed by third parties. These will be supported by selective disclosure of credentials.

HP has most recently argued for the implementation of 'Identifier-Based Encryption' (IBE) for use in health care. [136] Concerned with the enforcement of confidentiality and privacy in dynamic contexts, where people's roles and permissions are subject to frequent changes, HP proposes IBE over more traditional applications of cryptography such as PKI. Their system design requirements are

- *Privacy and confidentiality: messages need to be obfuscated by the system, at least till a legitimate user is*

entitled to de-obfuscate and read them;

- *Policy-based disclosure: disclosure policies need to be strictly associated to the obfuscated messages. The system must ensure that the disclosure of confidential information happens only if the associated policies (defined by the message sender) are satisfied;*
- *Strong authentication: people need to be strongly authenticated by the system. The system needs users' identities to decide if they are entitled to access obfuscated messages by retrieving their associated profiles (including their roles) and checking them against disclosure policies;*
- *Security: the overall system must be secure. Data need to be transmitted and stored in an obfuscated way;*
- *Flexibility: the system must allow users to flexibly specify policies to constrain the access to confidential information. (...) The system must allow users to obfuscate and send messages without knowing, a priori, the identity of the receiver. The system must support late-binding mechanisms for roles;*

IBE has two properties for these requirements.

- *Any kind of string can be used as an IBE encryption key (public key). Information is encrypted by using this string along with a "public detail", uniquely associated to a specific trusted third party, referred in this paper as trust authority (TA). This trust authority is the only entity that can generate the correspondent IBE decryption key. It only relies on a local secret that is a critical resource and needs to be properly protected;*
- *The generation of an IBE decryption key (associated to an IBE encryption key, i.e. a string) can be postponed in time. In other words an IBE decryption key can be generated (by a trust authority) a long time after the correspondent IBE encryption key was created.*

This creates a situation where it is possible to use the "role" of the intended email receiver as an IBE encryption key (public key) and directly encrypt a confidential email. Alternatively, the trust authority can also generate the decryption key when needed if the receiver is currently playing the requested role. There is no need to share or store any secret between the sender and the receiver. HP is working on testing this system in dynamic contexts such as government environments as well.

IBM, another RAPID collaborator, is conducting similar work in PIM. IBM has developed the Idemix system [137] that allows for minimal disclosure of information in an authentication transaction. The developers believe in the philosophy that data is best protected if not revealed at all, in a sense upholding the data minimisation requirement of data protection regulations, using pseudonyms and credentials rather than having to disclose actual certificates and unnecessary data.

[137] Camenisch, J., and Herreweghen, E. V. *Research Report: Design and Implementation of the Idemix Anonymous Credential System*. Zurich: IBM Research, June 17 2002. Available at http://domino.watson.ibm.com/library/cyberdig.nsf/papers/A056C698C02D9C8A85256BDE00524F61/$File/rz3419.pdf

IBM is also developing PETs for enterprises. Its enterprise privacy architecture (EPA) is able to identify how an organisation uses personal information at each business process level and identify possible areas of conflict with data protection legislation in a number of countries, including the EU. It consists of a Management Reference Model that manages the local privacy policy; and a Technical Reference Model that manages privacy at the transaction level through monitoring the collection and use of personal information. European government representatives have responded positively to the development of this architecture, according to IBM Research. IBM expects that the EPA will be used in government departments to monitor data management across agencies.

Section IV. Recommendations and Future Directions

The situation for Europe, privacy, and technology remains quite mixed.

Section I showed that a strong regulatory regime developed to harmonise the treatment of personal data within the European Union, and some remarkable legal developments. However there have been significant incursions on these rights and practices in the name of flexibility and national security that have proved worrisome. Most recently we have seen agreements established between the U.S. and the EU on the transfer of personal data of airline passengers well beyond the scope of reasonable requirements.

In section II we saw in some detail the national contexts of privacy and technology in Denmark, Finland, France, and the United Kingdom as each country adapts to the EU Directive of 1995, but also adapts to the incursions presented by data retention, national identification systems, e-government and joined-up databases, among other risks to privacy. To be fair, technologies are being developed within some of these countries, but these are hardly significant enough to match the risks presented by more recent government policies.

There was some sign of hope for the role of technology, as presented in section III. At the EU level a number of research projects and some European firms are developing technologies and practises to promote and enhance privacy rights. It is disappointing, however, that as the important policies are being formed, strategies are being implemented at the national level; the key technologies still remain years away. P3P may exist now, but doubt has been shed upon it by the experts in privacy in the EU as to whether it is truly a means to upholding the EU Directive. PISA appears to have never been completed; PRIDEH is quite simplistic; and GUIDES are merely best practices expertise, not self-enforcing, as technology is. PAMPAS and RAPID were signs of hope to some extent, but they are only Roadmap projects, signs of larger projects to come under FP6, and these projects may last up to four years. Hewlett-Packard, IBM, and Open Business Innovation and other firms are developing technologies, but the diffusion of their solutions may take equally long, and they have not yet been subjected to the scrutiny that P3P has received on their abilities to enforce data protection principles.

This last point on technological enforcement of data protection principles is most ominous. The fair information practices that are typically enshrined in data protection laws may sound like technical operations awaiting to be encoded into technology; but the reality is that they are highly socio-technological practices. That is, a key principle of privacy is data minimisation — limited purposes for data collections and limited collection of data. We saw that authentication technologies may support such a principle, but these technologies do not necessarily force the principle. Another key principle is informed consent: how can a technology enforce, let alone gauge, whether the consent of an individual was informed? Similarly for 'lawful access' of data, adequacy of purpose, etc. Privacy and technology may be intertwined, but we can not rely on either being the Trojan horse for the other.

The RAPID project summarised some of these key technology policy challenges succinctly, as

- *Negotiation of privacy between citizens and government is often impossible because of the mandatory character of providing data to government (obliged by law, in order to receive benefits etc.).*
- *An informational inequality often exists between governments and citizens. In the current climate of fight against terrorism and cybercrime this imbalance is currently shifting towards greater government control over citizen data.*
- *Data integration via interconnection creates blurry responsibilities. This implies responsibility for privacy consequences of projects and the problem of shared responsibilities in interconnected systems.*
- *How can we prevent the invention of new purposes? These are often based on flawed assumptions, including dangerous ones.*
- *The fundamental terminology is unclear. What is the meaning of "identity"; the implications of turning several identities into one (without questioning consequences); what are the different scenarios and contexts for identification?* [138]

[138] RAPID. Overall Roadmap 'Privacy and Identity Management' draft version 1. RAPID and IST, January 31 2003.

The PRIME and PAMPAS projects under the upcoming 6th framework of funding therefore have many socio-legal, economic, and philosophical issues to resolve.

There are certainly more optimistic viewpoints. In an interview, Pete Bramhall from Hewlett-Packard, presented the future scenario in a more uplifting light.

> *I am optimistic that enterprise-applicable PETs will be adopted by governments and industry, together with supporting technologies on the user side. But it will take a while, and need patience and long-term commit-*

ment and investment. I see privacy as similar to security and quality: initially regarded by management as an unnecessary cost and ignored, then grudgingly adopted after a nasty incident or when some direct benefit is pointed out, then seen as a potential for differentiation against competitors, then widespread, then harmonised. A long haul, but successful and worth it. As to which will succeed, the drive will come from regulation (at an EU level, more than nationally) and how this impacts enterprises and goverment agencies. I see users indirectly driving regulation, rather than particular technological approaches, and regulation influencing (but not specifying) the choices of implementation technologies. Economics and the market will drive standardisation.

Bramhall lucidly identifies a number of factors at play: economics and the market, regulatory regimes, the technologies, governments, industry, and most importantly, policy driven indirectly by 'users'.

In each country report there are signs that 'users', citizens, consumers, public-interest organisations, and public sentiments and concerns can drive national policy. The reality of data protection is that the principles are merely good points of departure, and they may be subverted under proposals like identification systems, joined-up government, cross-linking databases, and data retention. Even so, when educated the public can respond. Government policies can be shaped to minimise privacy threats, government policies can promote privacy protection, technological solutions can be researched and technologies can be adopted when there is enough of a compulsion. This compulsion will necessarily arise when 'users' are interested, and when 'users' make demands.

Indeed, the relationships among technology, policy, markets, government agencies, industry, and public opinion remain the topic of much academic controversy and debate. Further study is warranted; further action is required, from civil society, user groups, industry organisations such as the privacy architecture and infrastructure arms of RAPID and PRIME, government experts such as the Article 29 Working Group, to name a few. Technology is created mostly to enforce our understandings of policy, but successful technologies tend to be those that can be sold and implemented. There have been many great privacy enhancing technology solutions offered; and there have been nearly as many technologies that have proven to be market failures. Policies need to be linked tightly with public opinion and concerns of trust, privacy, and constitutional rights. Public opinion can be shaped, sometimes through education.

The environment in which we find ourselves today is economically and fiscally conservative, and one where public policy under duress. During the economic boom we all dreamed of new technological infrastructures and architectures being developed by innovative entrepreneurs because it was technologically feasible and sounded politically reasonable or at least interesting. We forgot about economic theories on adoption, we abandoned consideration of public wants and needs. Now as we develop technologies, as Bramhall notes, we must be patient. Similarly for public policy today: incursions are occurring on privacy rights because the opportunity exists and there appears to be a compelling need and sense of urgency. It is not entirely unreasonable to predict that this policy boom will also face a bust because the policy entrepreneurs are again failing to listen to the traditional arguments of public interest as well as constitutional and other legal protections.

Responsibility rests with governments to think progressively. Responsibility rests with the populace to ask much of their leaders and their policies, and to demand that expertise be provided on the options available. In the end, we keep on returning to the importance of the mass publics, public opinion, and public interests; educated by experts on privacy, shaping policy. This report outlines that there are currently and there are likely to be many technological options to pursue that may support protections of privacy. In this sense, the future is not bleak. It is just important that we do not place all our hope into regulation or into technology. A culture of privacy is the strongest protection, with strong regulators and representatives in government; and public opinion and expertise supporting the entire effort.