Privacy – Tomorrow’s Bottleneck in the Information Society?

Laurent BESLAY & Bernard CLEMENTS
JRC-IPTS (†), Seville, Spain

Introduction

The Problem of Privacy Protection

Since the emergence and global deployment of large scale IT systems in the late 70s and early 80's the issue of privacy has been an area of extreme concern, both politically and socially. The new economy and the emergence of new technologies to support it have done nothing to allay these concerns, quite the contrary in fact. The handling of personal data as an essential marketing tool in electronic commerce or the seamless interconnection of an infinity of electronic devices in the ambient intelligence networks of the future make the effective protection of such data seem difficult if not impossible to secure.

Overcoming the justifiable concerns of citizens – and the problems of trust and confidence that they raise in the public’s mind – represents a challenge to policymakers and to the private sector if the undoubted benefits of the new economy and the social benefits of new technologies are to be realised. In other words, it is in the interests of all concerned – suppliers and consumers alike – that a climate of trust and confidence in electronic ways of doing business be established at the earliest opportunity. Such a climate may be provided in a number of ways: ensuring the security and reliability of

(*) IPTS, the Institute of Prospective Technological Studies, is part of the European Commission’s Joint Research Centre. BESLAY and CLEMENTS are with the ICT Unit; they are grateful to colleagues Paula DIPIETROGIACOMO and Tom JACKSON for valuable inputs. Tom Jackson is with IPTS’ sister institute, IPSC (Institute for the Protection and Security of the Citizen). This paper is a modified version of a chapter in IPTS’ Report to the European Parliament ITRE Committee on Future Bottlenecks in the Information Society, June 2001. See http://www.jrc.es/FutureBottlenecksStudy.pdf for full text. The views expressed herein do not necessarily reflect those of the European Commission.
electronic payment systems is certainly one, guaranteeing the confidentiality of commercial communications is another. However, one of the most important in terms of public perception is the protection of personal data and privacy.

The question of privacy is however much more than a matter of making the new economy a viable substitute for the old. Privacy is inextricably bound up with each person's inalienable right to personal freedom, a prerequisite for all democratic and constitutional states (GUTWIRTH, 2001). The approaches to its management taken by policy-makers and public authorities will therefore fundamentally affect the nature of our democracy, and will determine the kind of society we would all wish to live in.

There are of course many different ways of defining privacy. One definition categorises the concept of privacy in three types (ROSENBERG, 1992):

- geographical privacy: the protection of the immediate sphere surrounding the person;
- personal privacy: the respect and the protection of the individual's mind and body;
- informational privacy: control of what personal data can be gathered, stored, processed or selectively disseminated, and how this should be done. Personal communication is included in this concept.

The emphasis in the present paper is on this latter aspect of informational privacy.

**Privacy and identity in tomorrow’s Information Society**

As Nicholas Negroponte pointed out, the Information Society is almost genetic in nature – each generation becomes progressively more "digital" than the preceding one (NEGROPONTE, 1995). The treatment of personal data is no exception to this process. Personal data today is increasingly dispersed in networks across organisations and frontiers and no longer simply resides in the controlled environment of well-defined monolithic databases. And just as information technology transformed business processes – and its partnership with communications technologies is now transforming commercial processes – privacy is undergoing similar radical change under the influence of these same technologies.
Today's determinants of privacy – name, address, telephone number, etc. – will in future give way to new "virtual" characteristics expressed in terms of a host of personal data (see figure 1). These increasingly sophisticated information technology applications and their potential to bring about radical change in our notions of privacy have raised growing concern among citizens about how their personal data is being used. Indeed, one view suggests that tomorrow, privacy "will be to the information economy of the next century what consumer protection and environmental concerns have been to the industrial society of the 20th century" (1).

This paper assesses whether these concerns are justified and if so, whether the increasing use of electronic expressions of personal data will create the need to redefine privacy indicators.

As in most areas of policy development, the measures to be taken will represent a balance between various interests; in this case between effective privacy protection, the economic and commercial environment, and the just needs of law enforcement authorities to combat crime and protect the democratic rights of citizens, without infringing those rights. Much of the following will demonstrate that, quite apart from the economic impact, clear social benefits will be derived for ordinary people through their adoption and take-up of new technologies and services. The potential for abuse has to be set against these benefits and a proportionate policy response formulated.

Policy responses will cover a range of technological, legal and extra-legal solutions. Technology represents an important component in the regulation of the Information Society, and in particular with regard to user privacy. The challenge is to develop laws that are as good tomorrow as they are today.

While Europe and some other countries have adopted a legislative approach, in the USA the private sector has taken a much more pro-active role. The private sector has an interest in promoting a climate of confidence in the use of its services and the desire to minimise regulatory intervention. As a result, self-regulatory mechanisms have been established through codes of practice and industry seal programmes. It is claimed, however, that for various reasons such schemes are difficult to enforce. Another more fundamental criticism is that they are based on legitimising commercial activities rather than on defending the basic rights of citizens, and lean too far in the direction of those interests as a result.

Structure of the paper

Several questions arise from the above analysis. The first is whether the current legal and regulatory environment, albeit recently updated, is sufficiently forward-looking to deal with the emerging threats to privacy. The second is the need to explore this new notion of privacy and to identify the points of vulnerability that will arise in the future. A still more fundamental question is whether the legal or regulatory construction created for the online world can be derived from an incremental adjustment of that previously established for the physical environment, or whether a completely new approach is called for.

We do not pretend to be able to answer these wide-ranging questions within the scope of a single paper; rather our purpose is to contribute to an on-going debate by signalling the issues at stake. We start by reviewing current regulatory approaches to privacy protection – legislative or self-regulatory – and developing a picture of their effectiveness in the face of increasing advances in the practices and technologies employed in the new economy. We then examine those advances in more detail, first with a medium-term perspective with a time horizon of around 5-years, followed by a longer-term perspective giving an idea of what kinds of new threats to privacy might arise in a brave new world of ambient intelligence, a go-anywhere/do-anything environment supported by a host of seamlessly interconnected devices, systems and networks. The paper concludes with a brief discussion of policy options that might be considered in order to deal with the emerging threats.
The Current Legislative and Regulatory Environment

International initiatives

Inspired by the need to preserve the free flow of personal data across borders, the OECD developed and issued privacy guidelines in 1980 in order to define good practice for the management of personal data, and to promote global adherence to basic privacy principles (2).

Up to this time, national rules on personal data protection had been established mainly to guard against the abuse of such data by the public sector which, in exercising the normal functions of government, was collecting large quantities of data about people (3). Since national rules protecting privacy were regarded by the private sector as potential constraints on economic activity, the OECD Guidelines were designed to both minimise and harmonise such rules rather than to enhance privacy as a specific goal of social policy.

The OECD Guidelines recognised the emergence of new information technology tools and the fact that personal data had by then acquired an economic value. As with international trade in any sector, there was a need to define a framework for the commercial exploitation of personal data in order to harmonise as far as possible the conditions for its use in different trading blocks. The OECD Guidelines, although entirely voluntary, therefore constituted an attempt to structure the terms of trade in personal data, and represented the first international consensus on the formation and application of privacy principles.

In 1981, the Council of Europe proposed a Convention on personal data protection, which came into force in 1985 (4). The text of the Convention focuses clearly on social interests i.e. the rights of the individual citizen. Unlike the OECD Guidelines, the Convention also represented an effective international legal instrument, requiring those nations party to it to pass domestic legislation implementing its terms.


(3) See, for example, the Data Protection Act of Hesse, West Germany, 1970; Sweden's Data Act of 1973; or that of France, 1978.

(4) Convention for the Protection of individuals with regard to automatic processing of personal data ETS no.: 108.
Here again, the implementation of privacy regulations was perceived by the private sector as a bottleneck for the (commercial) growth of the Information Society. The Convention was seen by regulators as a common reference and promotional tool for national legislation. The lack of implementation mechanisms, however, constituted its principal failure. The EU Directive that followed attempted to compensate for this weakness.

**European legislation**

Building on the OECD privacy principles, the EU has taken a proactive approach to the development of sound privacy practice within the Member States. Two EU Directives are currently in force:

- the general Data Protection Directive, adopted in October 1995 (5);

These legislative measures provide the European Union with a comprehensive legal framework for personal data protection.

It is worth highlighting the major principles of the Data Protection Directives which apply most directly to the issue of personal data management for on-line information systems:

- **Purpose limitation:** Data must only be processed for the specific purpose for which it was collected; it should not be further processed or passed on;
- **Data quality:** Personal data that is stored or collected must be correct and kept up to date;
- **Transparency:** Individuals should be informed of the reasons for which the data is collected and informed of the identity of the data controller;
- **Security:** Adequate security measures should be taken by the person controlling the data to ensure that it is not accessible by unauthorised third parties;
- **Access rights:** Individuals should be able to ascertain what information about them has been collected and how it has been processed, in addition to having the right to correct or modify the data, and where desired, prohibit it from being processed further.

---


Inspired by several major European initiatives (7), the Charter of Fundamental Rights of the European Union represents the biggest step forward in support of the protection of personal data (8). The objective of the Charter as expressed in its Article 8 is simply the respect and protection of the principle of privacy as a fundamental right, rather than one of finding the right balance between the privacy protection and the free flow of data.

Regarding the level of data protection, the Electronic Signatures Directive, which came into force on 19 January 2000, actually goes further than the main Data Protection Directive (9). Indeed, the Directive 95/46/EC does not prohibit the collection of personal data from third parties (Art. 11, para 1 S. 1). The Electronic Signatures Directive on the other hand prohibits the transmission of personal data, collected for the purposes of issuing and maintaining certificates related to digital signature, for any other purpose without the explicit consent of the data subject (Art. 8 para 2 S.2).

The emergence of digital signatures illustrates the balance between the need for strong authentication and the requirement for anonymity in privacy matters. In any event, the creation of a digital signature means that the user will have to provide to a third party copious amounts of personal data which will need to be well protected. The issue is then whether the certification infrastructure should be in the hands of a public or a private body.

The USA

The United States is widely recognised as being at the forefront of information technology but somewhat lagging in data protection. US legislation does not offer equivalent protection to that offered by the EU Directive; the US Privacy Act of 1974, for example, covers only the Federal public sector. No organisation or authority exists to oversee privacy protection or to act on complaints from data subjects about unfair or illegal use of their personal data.

In 1993, the Clinton/Gore Administration launched the National Information Infrastructure (NII) Programme, whose Task Force later developed privacy principles for all participants \(^{(10)}\). These principles offer guidelines only and do not have the force of law. To date, the US has strongly favoured self-regulation for the private sector; this approach places the burden of proof on the individual to demonstrate damage in the courts.

In response to Article 25 of the EU Data Protection Directive and in order to avoid problems for American companies in transferring their European data to the US, the US Department of Commerce reached agreement with the EU in July 2000 on International Safe Harbor Principles which provide self-regulatory privacy guidelines giving equivalent protection to that provided by the EU Directive \(^{(11)}\).

The Safe Harbor framework attempted to reconcile the different approaches to managing privacy protection on either side of the Atlantic. Its objectives are:
- to provide guidance to companies and other organisations in the US wishing to meet the "adequate protection" standard required by Article 25 of the EU Directive;
- to provide the necessary legal certainty for those adhering to the agreed standard, since compliance ensures that their data transfers will not be interrupted; and
- to create thereby a more predictable and less administratively burdensome framework, ensuring high data protection standards for data transfers from Europe to the USA.

The agreement on the Safe Harbour principles is intended diminish the risk that enforcement of the EU Directive might disturb US-EU trade and reduce the transaction costs associated with complying with the Directive. It is perhaps too early to judge the success, and certainly the effectiveness, of this first attempt at reconciling different legal and cultural environments within the same global economy. At the time of this writing, fewer than 40 US organisations, including just 12 companies, have signed up to the framework \(^{(12)}\). Even within the EU, the problem of converting the new legislation into effective business practice is currently exercising the minds of

\(^{(12)}\) www.ftc.gov
national data protection authorities. It should not be surprising therefore if its extension beyond EU frontiers is a similarly difficult task.

**Other trading blocks**

The question remains as to whether a common harmonised approach with other trading blocks will be possible. Cultural, political and historical differences have produced noticeable differences in the approaches taken by technologically developed states outside Europe in the setting up of information infrastructure programmes. Examples of the range of approaches are given below:

- **Singapore** was the first State to launch a national information infrastructure plan in 1991 \( ^{(13)} \). Though this island State tops the worldwide list in terms of Internet connections per household, it has no privacy protection laws. This is also the case in most other Asian states.

- **Japan**, on the other hand, is one of the very few Asian countries to have introduced a data protection act \( ^{(14)} \). However, this law applies only to national government organisations. Japanese policy favours a self-regulatory approach \( ^{(15)} \) to safeguarding privacy in the private sector.

- **Canada** has preferred to develop voluntary privacy codes and standards for business and industry associations. Indeed, the Canadian Privacy Act of 1982 applied to public sector bodies only (Federal agencies) and included the appointment of an Office of Privacy Commissioner (unlike the US legal initiative). In 1995 the Canadian Standards Association (CSA) started to negotiate a Model Code for the Protection of Personal Information in the private sector. As in the case of the US, this initiative was triggered by the EU Directive and the possibility of an embargo on the transfer of personal data transfer from Europe. It resulted in the Personal Information Protection and Electronic Documents Act that will enter into force in three stages from 1 January 2001 to 1 January 2004 \( ^{(16)} \).

\( ^{(16)} \) This Act was first introduced in the Canadian Parliament as Bill C54 in 1998, and reintroduced in 1999 as Bill C6.
The examples cited above underline the crucial impact of data protection initiatives on trade. The lack of an international supervisory mechanism for the Internet capable of enforcing legal obligations such as data protection means that the privacy issue will continue to have important implications for trade in the future.

Before the adoption of the 1995 EU Data Protection Directive, there was virtually no regulation which could, through its enforcement, raise an effective barrier to the free flow of data across the external borders of the Union. As noted, the entry into force of the Directive (July 2001), and in particular the reciprocity provisions of its Article 25, have spurred other countries into action in order not to prejudice their trading relationships with the Union. Canada, Hong Kong, the pre-accession countries of eastern Europe and others have established or are in the process of establishing privacy regulations broadly in the line with those of the EU.

Recent WTO agreements require that such measures do not constitute a disguised restriction on trade in services (17). However, Article XIV (c)(ii) of the General Agreement on Trade in Services (GATS) permits signatories to adopt measures to protect the privacy of individuals in relation to the processing and dissemination of personal data and the confidentiality of individual records and accounts.

Both the multilateral negotiations at the WTO and the US bilateral talks resulting in the Safe Harbor framework do, however, underline the need for a balance to be struck between the development of free trade and the protection of personal data. Electronic Commerce relies heavily on the use of personal data for the efficient marketing of goods and services, but in doing so it directly challenges well-established principles of privacy protection (18).

Two questions arise from this discussion:

1. Is the challenge to privacy imposed by current e-commerce practices effectively dealt with by the existing legislative and regulatory framework? If not, what are the areas of weakness?

---

(17) WTO – World Trade Organisation – Annexe 1B of WTO General Agreements, General Agreement on Trade in Services, Art XIV General Exceptions (c)(2).
(18) Ecommerce Business Impacts Project, final report to be published in the Autumn of 2001 by the OECD. IPTS is a partner in this project.
2. Will future developments in those practices, coupled with the application of new technologies, require new policies and legislative measures to be developed?

The following sections of the article address these points.

■ Adequacy of Existing Regulation

This section highlights the widening gaps which are appearing between the regulatory framework for privacy and common commercial practices in the on-line information business. It concludes that this is due in large measure to problems of implementation and enforcement of the existing legislation and describes briefly the nature of these problems.

Emerging gaps between legislation and commercial practice

Although the EU has a thorough legal framework for personal data protection defined by the Directives, and which has now been implemented as national law in most Member States, it is clear that there is increasing social anxiety with regard to the abuse and misuse of personal data within on-line information systems. For the most part, these concerns are not misplaced. An increasing number of risks and vulnerabilities related to privacy are being exposed, and on-line privacy abuses are increasingly reported in the media.

Despite the rigour of the Directives, criticisms have been raised that they are no longer in line with on-line information practices. It is argued that they were based on the privacy issues surrounding the management of large monolithic database systems, rather than the dynamic, highly-distributed data processing environment posed by today’s on-line systems. Through these systems, new privacy risks are emerging. They are linked particularly to technology developments in Internet browsers which allow user’s data, activities and interests to be tracked, profiled and monitored on an unprecedented scale.

Business and marketing corporations are able to build databases describing the surfing activities (such as the sites visited, products bought, search-engine queries made, banner-ads followed) for millions of on-line users. The collection of this data is largely facilitated using technologies
inherent within the client-side browsing tools (for example, cookies and HTTP handshaking protocols). This collection of this information is invisible to the user, and largely outside his or her control. With today’s powerful data-mining techniques, the information within these databases can be filtered to provide detailed profiles of individual users.

The question as to the relevance and validity of the existing EU privacy legislation has in fact been recently addressed by the Article 29 Data Protection Working Party (19). Their report presents reasoned arguments as to why the principles of the existing EU legislation have sufficient scope to cover most on-line data processing scenarios (20). However, there are a few emerging areas which do not fit easily within the scope of that legislation, and revision of the Directives may be necessary. In fact, in the case of Directive 97/66/EC revisions have already been proposed to keep it in line with rapid technology developments, and to clarify technical meaning in certain areas (21).

Irrespective of the scope and applicability of the privacy legislation, there are other fundamental limitations associated with a legislative approach to achieving a broad privacy compliant culture within the information society. The major difficulties lie in the area of enforcement of the legislation. As noted in the Article 29 Data Protection Working Party report, on-line data protection can only be sufficiently guaranteed if the existing legal framework is complied with. The following section addresses some of the existing limitations in regard to implementation and enforcement of the Directives.

Detection and monitoring of privacy abuses

Monitoring of compliance with the data privacy legislation is the responsibility of the national Data Protection Agencies, who fulfil both an advisory and surveillance capacity (22). However, detection and monitoring of non-compliant privacy practices is a particularly difficult challenge, especially given the pervasive nature of on-line information management systems and the exponential increase of e-commerce. It is also extremely

(19) The Working Party has been established by Article 29 of Directive 95/46/EC. It is the independent EU Advisory Board on Data Protection and Privacy. Its tasks are defined in Article 30 of Directive 95/46/EC and in Article 14 of Directive 97/66/EC.
(21) Reference needed here.
(22) See http://europa.eu.int/comm/internal_market/en/media/dataprot/links.htm
difficult for end-users to identify or detect instances of personal data abuse, particularly as most of the technologies used to monitor or profile individuals are invisible to the typical Internet user. The marketing of personal data that has been collected on-line, an increasingly common practice given its economic value to third parties, is also an activity that is invisible to the user. Similarly, data aggregation and data-mining of user profiles is an activity that is conducted off-line by third-party organisations generally unknown to the user. Even in those cases where an individual may suspect an abuse of their personal data it can be an almost impossible task to trace those responsible, or to gain rightful access to the data relating to them held on-line.

In these instances, the Data Protection Agencies are the primary point of recourse for the individual. There have been proposals for the development of on-line automated privacy dispute resolution schemes to manage these issues, but, as yet, there is no significant EU infrastructure to support these ideas. Some Member States have made proposals for the development of specialised sections within law enforcement agencies dealing specifically with on-line issues. Whilst such groups may have a role to play in privacy enforcement it is more likely that the resources of these units will be largely assigned to manage cyber-crime (e-fraud, paedophilia, etc.) rather than privacy issues.

One alternate mechanism for compliance enforcement is third-party accreditation or audit schemes which can offer on-line 'trust-seals' to indicate a privacy compliant organisation. Examples of trust-seals are the 'WHICH web-trader', ISEC, TESTAANKOOP, BBB, and TRUSTe web certificates (23). However, despite the inherent value of this principle, there are widely-documented cases that sites exhibiting such seals have continued to misuse personal data for marketing or other commercial purposes, contrary to their stated policies. The trust-seal organisations have been shown to be largely ineffective in preventing or detecting such abuses, and have no real powers of sanction in these cases.

Proposals for a European-wide certification scheme have been proposed and investigated within the EU. However, no practical implementation or infrastructure has been proposed as yet. Until such schemes or alternative measures are implemented, users will remain in a vulnerable position with little to no transparency in regard to how their on-line data is being processed or distributed.

Technology requirements

Some aspects of the Data Protection Directives are ambitious in their scope, particularly regarding the principles of data access and transparency. Whilst the Directives are technology neutral in regard to the principles, it is clear that compliance raises requirements for advanced technology solutions for privacy management. For example, technologies for digital signatures, anonymity, data encryption, trust-seals, authentication and authorisation may all be required in order to implement privacy-compliant business processes. However, many of these technologies have not yet reached mature market status. Consequently, there is not only a lack of integrated systems solutions for privacy-compliant processes, but also clear technology gaps in the market and particularly a lack of mature, coherent infrastructures across the EU markets to support them. For example, there is as yet no pan-European Certification Infrastructure to support digital signatures.

Awareness

European industry and the commercial sector are obliged to conform to the data protection requirements laid out in the EU Directives. However, in a recent UK survey carried out by GB Information Management consultants (24), it was stated that nine out of ten businesses in the UK were not aware of the implications of the personal data protection legislation. This is not a failing limited to the UK, but can be generalised across much of Europe. Far greater awareness of the legislation is required in all EU business sectors, although the mechanisms for achieving this are not yet clear. The Data Protection Agencies are possibly under-resourced for the scale of the task.

The European Commission has asked the European Standards bodies to consider the case for standardisation in support of the data protection legislation. Such standardisation would help businesses to align the practices with the requirements of the Directives, and also facilitate the work of the Data Protection Agencies in securing compliance. Achieving consensus on a standards approach is the main obstacle to progressing this work, although CEN/ISSSS is actively pursuing the task and will shortly put out proposals for public discussion.

Conclusions

The EU has a comprehensive and rigorous legal framework for protection for personal data. However, privacy abuses continue on a vast and persistent scale, largely due to the problems of enforcement of the legislation, detection of non-compliant practices, and gaps in privacy enabling technology. Related problems are the perceived lack of a clear business case for organisations to invest in privacy compliant business processes and systems, and the relatively minor risk of penalty or sanction incurred should data abuses be detected.

Emerging Trends Involving Personal Data

Having looked, in the previous sections, at the current regulatory environment protecting privacy and its adequacy, the following examine the medium and long-term prospects for privacy protection in the light of technological, commercial and administrative (i.e. public service) developments. A review of emerging technologies supporting or threatening privacy protection is followed by a description of the kinds of services enabled by those technologies. These include emerging services using mobile communications for locating individuals and places, and new practices in electronic commerce which can pose a threat to privacy.

It is perhaps worth restating that since this report focuses on privacy protection, it takes a critical and even pessimistic view of such threats. The discussion does not therefore stress the very positive benefits that the services described can give to users and citizens, and these should not be ignored in any policy analysis. One case in point is described in the subsection on healthcare data – the application of emerging information and communications technologies to improve health services far outweighs the potential misuse of healthcare data if appropriate technological and legal measures of protection are implemented.

PETs & PITs - Technologies having an impact on privacy

The graphic acronyms PETs (Privacy-enhancing technologies) and PITs (Privacy-invasive technologies) serve to classify emerging technologies in terms of their effect on privacy. Although the raison d’être of PITs is to deliver a customised service to clients rather than the invasion of privacy for
criminal purposes, this latter consideration has led to the development of systems capable of providing a high level of personalised service, whilst requiring that the collection of personally identifiable data be kept to a minimum.

**PETs (privacy-enhancing)**

PETs are technologies which may be used to improve the security of personal data. Such technologies may have been expressly developed for this purpose (e.g. encryption) while others have inherent security features.

One example of both types is embodied in Virtual Private Networks (VPNs) (25). These are partitioned sections of a public network dedicated to particular corporate users, and they enable public operators to offer companies an alternative to deploying their own private networks. The compartment of the network reserved for a particular user is protected by a so-called ‘firewall’ which restricts access to authorised users. The transmission components of the networks (bridges, routers, etc) use encryption technology to further enhance security. They also perform address translation; satisfy requirements for strong authentication; and serve up real-time alarms and extensive logging. Software-based VPNs are ideal in situations where both endpoints of the VPN are not controlled by the same organisation (typical of client support requirements or business partnerships), or when different firewalls and routers are implemented within the same organisation.

Peer-to-peer (P2P) technology also has the potential to enhance privacy, as tracking will become proportionally more difficult with the non-intervention of servers. Mass information stored on common servers is vulnerable in a way that locally-stored individual information is not.

The Platform for Privacy Preference Project (P3P) is a standard of the World Wide Web Consortium which focuses on privacy practice disclosure with respect to data collected through web interactions with merchants (26). It has been designed to help users reach a semi-automated agreement with on-line merchants regarding the processing of their personal data. It does not exclude the use of other privacy technologies such as encryption or web anonymisers.

---

(25) VPN stands for Virtual Private Network. VPNs provide an encrypted connection between a user's distributed sites over a public network (e.g., the Internet). By contrast, a private network uses dedicated circuits and possibly encryption.

(26) See http://www.w3c.org/P3P
PITs (privacy-threatening)

While the privacy-enhancing features of firewalls were listed under PETs, protection technologies based on firewalls do have some shortcomings. The main problem is that their use assumes the existence of a capability to identify, define and characterise the extent of administrative control over a system, the access points to that system, and all the signals that appear at those access points. In unbounded systems such as the Internet, this kind of information cannot be easily determined.

Interactive Digital Television (DTV) is also raising privacy concerns as operators seek to target their programme offerings by tracking the viewing behaviour of their customers. This is similar to the profiling problems of Internet use described earlier, and will increase the potential for privacy invasion in what was hitherto a one-way broadcast system. Household interests can therefore be captured and tracked, exposing the user to unwanted targeted online advertisements or to unauthorised disclosure of such interests to third parties.

Other technologies

A number of technologies are now rapidly being deployed to enable wireless, mobile computing via LANs, VPNs access to end-user devices such as mass-produced handsets (PDAs and cell phones), and embedded devices. Wireless protocols such as WAP, WTLS, Bluetooth, GSM, wireless LAN (IEEE 802.11), VPN and mobile IP all have built-in security functionality but as their usage is not wide-world to date, privacy related weaknesses have yet to be identified. We explore this point later in the report.

It is expected that mobile code-based applications (JAVA, ActiveX, Mobile Agents) will be intensively developed and used for WAP and third-generation mobile (UMTS) applications, including localisation services. These are described below.

Localisation services

Localisation services exploit the premise that information gains added value and relevance if it is closely related to its location. Indeed, applications that use localisation information will be able to adapt their services to the
environment and deliver to users data that is relevant to their current situation.

For the purposes of this study, we will consider two main technologies which provide localisation information: satellite systems and mobile communications networks. Localisation services are at the beginning of their lifecycle, but it is recognised that they represent a huge potential market. According to the technology research company IDC, the market for localisation services is estimated at nearly €600 million and is forecast to approach €5 billion within three years (27).

Satellite systems have been used for geographical satellite positioning services for over twenty years. The US Department of Defense (DoD) has provided its Global Positioning System (GPS) free of charge, initially with decreased accuracy for civilian usage. The decision to increase its resolution came only days before the official announcement of the competing European project, Galileo, underlining the commercial potential of these services. Companies seeking to tap this commercial potential are installing wireless location systems in vehicles, hand-held computers, cell phones, watchbands, and even in a chip that can be inserted beneath the skin so that a person’s location can be pinpointed anywhere.

Positioning services based on mobile communications networks are now being provided by mobile operators. They use a variety of methods to provide location-based services to an increasing number of mobile phone users (28). Such services are expected to be an integral part of future mobile networks. Because they are linked to the mobile phone market, localisation services will become within the reach of millions of users, opening a Pandora’s box of problems related to privacy.

Two main issues arise which are important for privacy. The first is the absolute localisation of the user, i.e. co-ordinates of the location, which could be defined as “where you are”. This service already has commercial, law enforcement and emergency applications:

- In the US, a Federal mandate requires all wireless companies to be able to pinpoint the location of a wireless 911 (emergency) call by October 2001 (29). By this date all mobile phones will be equipped with advanced wireless tracking technology. Though this initiative was launched for

(28) The different methods are: Cell of origin, Signal strength, direction of arrival, time of arrival.
commendable reasons, there is, as yet, no regulatory framework to prevent the system being used for undesirable purposes by private organisations. It is easy to imagine insurers, for example, making use of information that a particular client participates in dangerous sports, or is being treated for AIDS at a local specialist clinic.

- With this Federal obligation, the FCC has also enabled a host of new commercial applications. Mobile operators can now offer driving directions, local news, traffic delay updates, weather, etc. NTT DoCoMo has a 'Friends Finder' service, which provides the location of users to their friends. Though this last application offers a security feature enabling the user to define those persons allowed to see his location, there is no legal obligation for it to be provided and there is no standard or minimum requirement for its definition.

- Law enforcement agencies use localisation information to catch criminals. In most cases this useful new tool is controlled by a court warrant. Nevertheless there is still no agreement on the conditions of use, nor any mutual recognition agreement for its legal value as digital evidence.

The second issue is the proximity or relative localisation of the user, i.e. what located objects are nearby, which could be defined as "near to where you are". Relative localisation gives rise to "push services", where unsolicited information is sent to the user. For example, it is believed that British Telecom is testing a third-generation (3G) mobile network in the Isle of Man in a partnership with McDonalds to provide push services. When users come near to one of these well-known eating establishments, they will no doubt receive messages of a promotional kind encouraging them to stop by for a meal. To encourage the use of 3G wireless phones, service providers have already made business plans which would give users free calls in exchange for receiving numerous location-based advertisements per day. Here 'privacy' is clearly conceived as a commodity in which the user and the service provider enter into a negotiation regarding its exchange. Privacy then shifts from being a fundamental right to a good to be exchanged or sold for value-added services.

The potential use of localisation services by third-generation wireless phones points to several critical privacy issues. This new generation of mobile services will offer fast access to the Internet, a borderless environment from a regulatory standpoint, and will simultaneously provide enhanced localisation services. The concerns regarding the profiling of Internet users described earlier in this report will take on added significance when combined with information on their physical whereabouts.
The use of proximity localisation could also serve to inform users of a friend’s presence nearby (30). Future mobile systems carried by individuals, when enhanced by powerful 3G wireless technology, could exchange information automatically with other nearby systems. It will then be necessary to have the ability to control the extent to which information (especially personal data) can be automatically exchanged, and under what conditions.

Localisation services have a great potential for benefitting citizens and this market sector is expected to grow dramatically. At the same time, they greatly challenge the integrity of individual privacy. Clearly, it is in the interests of service providers that their potential customers have confidence in the systems to respect their privacy, otherwise they will not engage. The potential market for these services will only become a reality if user privacy is demonstrably preserved.

Emerging E-commerce practices

The Internet and the world-wide-web have created unprecedented opportunities for global interaction - for business, for social services, for recreation, and have seen the establishment of a new set of on-line business activities described collectively as e-commerce. The estimates for the growth and potential of e-commerce are vast, and market predictions indicate that it will be a trading sector with a turnover of €340 billion within the EU by 2003 (31).

However, the same Internet technologies that have facilitated the development of e-commerce have also created a new regime of privacy risks for consumers. It is now possible for the on-line activities of an individual to be monitored, tracked and recorded in great detail, posing considerable threats to individual privacy. The deployment of powerful data mining and data collection technologies mean that it is entirely feasible for commercial organisations to create and manage databases containing the personal data and activity profiles for millions of on-line users.

The primary motivation for companies to create these databases would appear to be for marketing purposes, either for targeted mailing or

(30) Yahoo! Europe and CellPoint Systems AB announced that they have signed an agreement to co-market a person-to-person locator service for mobile phones, 4 May 2000.
'customised' services at on-line stores. However, privacy advocates have argued that there may be more sinister reasons behind the collection of the data, such as credit profiling or health screening by insurance companies (32). In the following sections the technologies that can facilitate on-line privacy abuses are described, and the nature of the risks is elaborated.

**Cookie Files and Privacy Risks**

One well-known technology that is at the core of many on-line privacy abuses is the 'cookie'. The HTTP cookie is a file mechanism that creates the opportunity for more automated interaction between a web server and a client - it provides the remote server with a 'memory' of a user's identity. The contents of the cookie file will vary depending upon the type of website visited, but it will typically store information about a user's personal data, such as name and location, and their recent, common or preferred activities on websites. It may also be used to store information relating to credit cards, or site passwords. In addition, it can provide some automation or 'intelligence' in e-commerce applications such as 'shopping carts' and management of user preferences.

Cookies constitute a powerful technology for enhancing website interactivity. However, they can be misused in ways that present a risk of abuse to personal privacy:

- **Security failures**: Sensitive information is often stored in cookie files (passwords, credit card details, etc.) which are passed openly over the Internet. The contents of a cookie are, in theory, accessible to anybody capable of intercepting a cookie on the Internet or maliciously gaining remote access to a networked computer. While cookie files should be encrypted when containing personal data, users have no control over the security measures being taken with cookie file transfer and storage.

- **Monitoring**: Many people believe that user identification via cookie technology is an invasion of their personal privacy. People are at liberty to enter a retail store in the physical world with anonymity and without their purchases or activities being recorded or monitored. Privacy advocates feel that the same choice for anonymity should be available during on-line

(32) One case demonstrates that the concerns of privacy organisations may be well-founded; a US supermarket chain used a client's purchasing information stored via his store 'bonus' card to claim in a law suit that his regular purchases of alcohol suggested he was an alcoholic. The Times, Online Special: Internet Privacy, April 10, 2000, http://www.the-times.co.uk/onlinespecials/britain/privacy/
browsing. Cookies may also permit a third party to investigate the activities of an individual if they have access to their computer and their cookie files. This raises far-reaching issues. For example, if a site administrator maintains records of an individual's activities or presence at a website, would Government or prosecuting authorities have the rights to access those records to be used against that individual in a court case?

- **Data Disclosure**: A site that has personal information about an individual, stored via cookie technology, may exchange this data with other sites (for example, related business partners or sites that buy advertising space from them). Such sharing of data may extend as far as cookies being 'synchronised' for a group of businesses. This implies that personal information supplied voluntarily at one site may be used to track or identify an individual at other sites where they have never intentionally disclosed such information.

- **Limited control**: End-users have very little control over the content and use of cookies; in fact to most users they are a totally invisible technology. Some web browsers provide the user with an option to disable cookies (i.e. to not accept them) however, this can often make some sites totally inaccessible. For those who do decide to accept cookie files there are no browser mechanisms that inform the user as to what use is being made of the cookie or what data is being stored within it.

**Online user profiling**

Profiling is a business concept from the information brokerage sector. It is the name given to the process of building databases that contain the preferences, activities and characteristics of clients and customers. It is a practice that has long been part of the commercial sector, but which has developed significantly with the growth of e-commerce and the Internet. It is quite common for the profiling databases to hold references to millions of web clients. Many commercial websites (including many of the on-line search engines) have associations with commercial information brokerage companies.

These sites make use of cookies to monitor a client's activities at the host site and record the data provided to the web server. Users’ interests, browsing patterns and buying choices are stored as profiles in a database. This profile information is used to decide which advertisements or services will be offered at the affiliated websites. The information is typically collected and stored without a user's knowledge or, more importantly, consent,
although it is purported to be not personally identifiable. However, where a client/customer provides personal data to a web server (e.g. name and address) it is possible for the data to be correlated with e-mail addresses, IP addresses and demography, to create a far more personalised profile.

Organisations involved in these activities stress that profiling activities are in the interests of consumers; providing more customised and directed services through the web. On the other hand, the practice is seen by many as a violation of basic privacy rights because data is collected and distributed without a user’s consent. Mechanisms for ‘opt out’ whereby a user can decide when and where they want their data to be collected and processed are being discussed by many information brokerage agencies (33). The W3C standard, Platform for Privacy Preferences (P3P), described earlier in this section, is an example of a technology facilitating this. However, many privacy organisations are demanding that an ‘opt in’ policy should be the norm, whereby users are given the freedom to choose anonymity over profiling.

**Tracking**

When an individual is browsing on the world-wide-web the paths that they take from one site to another can be monitored. In fact, many commercial on-line organisations trace and store a consumer’s route to their site. This is achieved through the use of the HTTP server variables - a set of values that are, by default, passed between the client and host web server during any log-on to a site. From just these default variables it is possible to identify the user name, domain and geographic location (from the DNS and IP address), operating and browsing environment, as well as the URL location visited prior to the current web site. A user cannot disable this HTTP ‘chattering’ process.

**Invasive processing**

In addition to the browser mechanisms described above which permit the collection of personal data, there are also privacy threats posed by new programming paradigms. Powerful programming languages have been developed for web-based applications, and these have greatly increased the

---

(33) The terms ‘opt-in’ and ‘opt-out’ are used in privacy debates. ‘opt-out’ describes a scenario whereby an individual is assumed to be included in a scheme unless they explicitly state otherwise. ‘opt-in’ describes the scenario whereby an individual is only included in a scheme if they give their explicit request.
complexity and capability of the Internet. The languages include Java, JavaScript, XML, and Active X. They permit remote servers to run applications on a client’s PC, via the web browser. Many of these languages have security gaps which make it possible for programmers to create malicious software that exploits loopholes to gain access to a remote networked machine. However, these languages are also being exploited in the commercial sector to allow organisations to gain access to a consumer’s personal computing environment and the data held within it.

A well-documented example of this type of invasive processing activity was identified in connection with the widely used Realplayer tool (34). Realplayer is a freely downloadable multimedia player for PC platforms. However, registration requires submission of personal data. In one particular release of the tool the details of any media content (e.g. MP3 music files) played on the tool were relayed back to the Realplayer organisation (invisibly to the user) so that a profile of the user’s listening preferences could be built up. Once this feature had been discovered there was a major consumer reaction against the suppliers of Realplayer, who subsequently disabled the hidden mechanism in later releases, and have made it an ‘opt-in’ feature. Typical end-users are totally unaware of the privacy risks that may posed by Internet enabled software applications running within their computing environment.

**Conclusions**

The data collection and monitoring practices described above are becoming widespread in the e-commerce sector. They are generally justified under the guise of the trend towards personalisation of the services at a website, described by the sector as ‘one-to-one’ service, for data marketing reasons. However, in general such practices, where the data is collected or stored with a user’s consent, are contrary to the principles of EU Data Protection legislation, most notably with regard to the articles relating to legitimacy of data collection and fair processing. The legislation has not yet had sufficient impact to deter or prevent such practices. It is likely that the profiling of users and the third party processing of data (without user consent) will continue until measures for enforcement of the legislation are strengthened. An alternative scenario is that consumer reaction to these practices may be sufficiently strong to motivate the e-commerce sector to introduce self-regulation and data protection compliance voluntarily.

(34) See http://www.real.com
Healthcare data

One of the clearest examples of how the move to the on-line digitisation of personal data can create whole new areas of privacy risks can be seen in the Health Sector.

As personal health data touch upon the identity and private life of the individual they are extremely sensitive; these data are considered to "form part of the personality of the individual", and cannot therefore be treated as mere objects of commercial transaction (35). Patient healthcare records, traditionally held on paper records, are now being stored and processed in centralised on-line information management systems within healthcare organisations. Records that were once stored locally in filed reports are now available on a much broader basis as hospitals and healthcare organisations adopt Hospital Information Networks (HINs) in a bid to automate and streamline their information management systems.

This section examines some of the implications of the increasing reach and coverage of personal healthcare data, and the attendant risks of unauthorised or undesired access thereto.

The widening range of stakeholders

The fact that the files are available on-line has meant that a much broader range of 'stakeholders' in the health sector business chain are now seeking access to patient data. For example, pharmaceutical companies, health insurance companies and banks, research centres and regional health authorities are now being linked into the 'health chain' process via HINs, and all these organisations are staking a claim on access to patient data, and, in many cases, being granted that access. The confidentiality of patient data is substantially undermined in these new networked scenarios, for two principle reasons:

- A patient no longer has control or visibility of where their clinical data is being transferred. Whilst the Hippocratic Oath has governed hospital ethics regarding patient confidentiality for many centuries, this same ethic is not prevalent in the business sector. Consequently, with the increased distribution of health data comes an increased risk that a third party can misuse that data.

• There is an inherent security hazard associated with transferring files over the Internet that can lead to breach of confidentiality. The security of the networks that are typically being used can be compromised, either maliciously or inadvertently, such that information leakage can occur. The more widespread the health networks become, and the greater the numbers of third party stakeholders which interact with these networks, the greater the potential for security breaches. This is particularly the case as the data spreads further away from the core healthcare infrastructure, where security mechanisms and infrastructures may be much more rigorous of those than say a health insurance agency.

The development of HINs and networking of third party organisations has not yet reached the point where it is commonplace. However, there are already well documented cases of breaches of patient record confidentiality that have arisen from the move to digitised healthcare records. Several alarming cases were reported in a recent ruling issued by the US Government (see Text Box 1) (36). Indeed, the public concerns over the confidentiality of patient medical records become all the more pronounced when third parties have a strong interest in gaining access to personal health data which is recorded and stored electronically.

Text Box 1: Examples of breaches of patient record confidentiality in the US

<table>
<thead>
<tr>
<th>Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>A banker who also sat on a county health board gained access to patients' records and identified several people with cancer and cancelled their mortgages (37).</td>
</tr>
<tr>
<td>A physician was diagnosed with AIDS at the hospital in which he practised medicine. His surgical privileges were suspended (38).</td>
</tr>
<tr>
<td>A candidate for Congress nearly saw her campaign derailed when newspapers published the fact that she had sought psychiatric treatment after a suicide attempt (39).</td>
</tr>
<tr>
<td>A 30-year FBI veteran was put on administrative leave when, without his permission, his pharmacy released information about his treatment for depression (40).</td>
</tr>
<tr>
<td>Consumer Reports found that 40 percent of insurers disclose personal health information to lenders, employers, or marketers without customer permission (41).</td>
</tr>
</tbody>
</table>

(36) Standards for Privacy of Individually Identifiable Health Information, Department Of Health And Human Services, Office of the Secretary, 45 CFR Parts 160 through 164, Rin: 0991-AB08, Dec 2000. http://aspe.hhs.gov/admsimp/final/PvcPre01.htm
(38) Estate of Behringer v. Medical Center at Princeton, 249 N.J. Super. 597.
(40) Los Angeles Times, September 1, 1998.
The increasing use of genetic data

Other public concerns and possible bottlenecks relate to the effects of globalisation on the gathering of statistics on health and the way population profiles to express those statistics. Standards relating to such statistics are not neutral; they embody the ethical, social, political and epistemological choices of their creators, and will necessarily favour particular views of patients or diseases while excluding others (42).

Currently, legal standards for the protection of the citizen in healthcare differ from country to country, and the diverse nature of healthcare management in European countries has given rise to a particularly disparate array of legislation relevant to ICT and healthcare across the continent. In spite of the massive flows of health data inside and outside Europe, no specific binding legislation exists to address the particular issues arising from the use of these data in the emerging Information Society.

The handling of health-related databases is a good example. A recent OECD Working Party Report recognised that there is a need for policies, practices and procedures for handling electronic health information databases that take into account privacy issues and the vulnerabilities of health information in computerised form, of electronic handling of data, and of network systems (43). Although the need for "appropriate technical measures" to protect health data is cited in all current guidelines, little progress has yet been made in clarifying what the term "appropriate" should signify and how to achieve this goal in practice (44).

The concerns are particularly relevant to the handling of genetic data, in view of the important expansion of human DNA sampling and data...

(42) The popular term is 'statistics', we really mean data. Standards here refer to the methods of gathering and expressing such data. To quote from the European Group on Ethics in Science and New Technologies 1999 report, Ethical Issues of Healthcare in the Information Society, "Standardisation is inherent to the digitization of health data. Even more so in the healthcare sector, where classification and coding (clinical protocols, diagnostic related code, checklists, etc.) are in widespread use. As these standards are not neutral, but embody value-related choices, they must be transparent and subject to evaluation by independent bodies (for example, ethical committees, patient organisations and professional associations). Moreover, personal health data may be used to construct profiles of a patient as a basis of health policy decision-making."


collection (45). At present there is no official census of genetic banks with regard to their number, the kind of biological material stored, the services available, as well as their financing. Whether samples are identified, coded or anonymous, the banking of genetic information raises serious issues pertaining to access, informed consent, privacy and confidentiality of genetic information, civil liberties, patenting and property rights.

A key concern is whether unauthorised third parties may gain access to genetic profiles or to the results of simple DNA tests. Although DNA databanking is progressively part of medical practice, there is no consensus about how to manage and organise collections of human material for genetic studies. DNA banking practices raise economic and legal issues and it appears necessary:

f) to control the flow of banked DNA and DNA data;
g) to develop policies to regulate DNA banking more closely;
h) to insure that DNA banking can perform its functions without impinging on the rights and interests of individuals who have their DNA sample or DNA data in a such a bank (46).

The role of technology

The above examples demonstrate that the networking of healthcare organisations and the electronic transfer of patient health data are leading to an erosion of the controls over confidentiality. It is highly unlikely that the trend for networking within healthcare organisations will be reversed, in fact it is only likely to increase with growing commercial pressures to improve the business efficiency in these organisations. Consequently, the technology requirements for the protection and privacy-compliant management of patient healthcare records need to be investigated in detail.

Two key technology requirements are immediately apparent; the need for secure access control to patient data, and, in those cases where there may be legitimate reason for clinical data to be passed to a third party (for example, for clinical research purposes) the need for ‘anonymising’ the corresponding electronic records. Whilst these are ongoing research areas

(45) New DNA samples are being collected in the US at the rate of 20 million a year. See: E. Eisemann, "Stored Tissue Samples: An Inventory of Sources in the United States" RAND Critical technologies Institute, 1999.
(see for example van BLARKOM 1998), there are as yet no definitive systems solutions or standards in this field (47).

Conclusions

In summary, the networking of health-care information systems is leading to the same privacy vulnerabilities that are witnessed in other IT-enabled activities, such as electronic commerce. However, in the case of patient clinical data the vulnerabilities seem to be all the more acute given that there has traditionally been a culture of confidentiality and trust implicit in the treatment of health records. Networked healthcare systems are leading to the increasing distribution of patient data, which is leading to lapses in confidentiality that have significant detrimental consequences for individual patients. The economic drive for networking and streamlining of health-care information systems, and the implementation of HINs, is pushing ahead despite the quite clear technology gaps for providing the required secure and confidential infrastructure that is vital in this highly sensitive data arena. Stronger legislation enforcement, stronger technical standards and stronger technologies are all required in this sector, to halt the rapidly escalating risk of erosion of guaranteed and expected patient data confidentiality.

Moreover, the adoption of a Directive on medical data protection is considered desirable within the framework of the current Data Protection Directive. In fact, although Art. 8 of the Directive 95/46/EC includes reference to health data as "sensitive data", many questions remain to be defined, including:
- the definition of legitimate uses and users of personal health data;
- the user’s duty to confidentiality equivalent to a professional duty of medical secrecy;
- users’ personal accountability for the data uses;
- citizen’s rights to oppose the use of their data for secondary purposes.

Criminal abuse of personal data

A definition of the ‘abusive’ use of personal data is crucial to the privacy issue. This definition could be based on a classification of user behaviour and on the nature of the new technological environment. Criminal abuse is

made possible by the conjunction of three factors: motive, opportunity and vulnerability. When value is sufficient to incite motive, the influence of the two other factors depends specifically on the available technologies - in the case of personal data, on the availability of new information and communications technologies (ICTs). The scramble to obtain valuable personal data in the Information Society could be compared to the gold rush in the Wild West. Due to the lack of a clear regulatory framework and a host of technical vulnerabilities, the number of opportunities and the motives are great.

Two groups of users are identified in this process – those who have an authorised or legitimate purpose for the use of private data, and those who abuse that data. Because of the complexity of the digital environment, it is necessary to further divide the abuser group into two subclasses:

- Those who make abusive use of information within the current framework. This case is well illustrated by a French resident who uses a British airline company to travel to a South American country. He pays for his plane ticket with a credit card, and receives insurance provided by a US insurance company. In this case, the collection of personal data will be subject to very different legal frameworks, and there is a strong possibility that some of the processes involved may be considered as illegal by some and legal by others.

- Those who make abusive use of personal data for illegal or unethical purposes represent the second subgroup. According to A Cavoukian, the danger of criminal abuse of personal data isn't so much an Orwellian Big Brother, but rather the more insidious presence of numerous "little brothers" (CAVOUKIAN & TAPSCOTT, 1996). For reasons connected with cultural social and economic factors, the level of this threat to privacy is difficult to estimate in a digital world. Nevertheless, a person’s reaction to someone entering his house, taking notes on the size of his shoes, trousers, the brand of the toothpaste and medicines he uses, and listing the things he owns, is different to when the same investigation is carried out digitally by a well known credit card provider. In both cases, the added value gathered is generally the same and may well be more in the case of digitally-collected information, as this method facilitates the gathering of dynamic and up-to-date personal information.

One of the main principles of the privacy concept is "the right to forget". This right demands that cumulative personal data be erased after it has been used for the purpose for which it was stored. The largest Internet search engine recently bought a company that has owned and operated a
Usenet Discussion Service (a database of thousands of discussion forums) since 1995 (48). After the conclusion of a financial transaction, the user’s chat forum collection is copied and pasted into the database of the search engine company. Because these chat forums are still publicly accessible, a candidate for a job, say, could potentially have to deal with comments he made years ago during his or her youth. The concept of limited storage time for personal data was included early in European regulatory initiatives, but it needs to be used with care as a privacy-enhancing tool (49). Indeed, for this principle to be properly applied, it would be necessary to structure and trace more accurately the source and the collection date of the personal data, which would, in turn and in itself, pose a threat to privacy.

The digitisation of information leaves the field of personal data wide open to abuse. In the digital world every economic, social or administrative transaction creates a trail of digital data, data which was previously private. Except for some specific transactions, particularly those with government bodies, the mountain of data generated has never been protected by legal or ethical measures. Therefore, the creation, storage and dissemination of multiple digital records constitute the main activity of this new environment. Two of the natural laws of the digital new world have a direct impact on the growth of criminal abuse of personal data:

• Digital records are inherently reproducible. Indeed, one of the virtues, but also one of the vices, of digital records is that they can be endlessly duplicated, in copies indistinguishable from the original. The dissemination of personal data, uncontrolled by its owner, is then greatly facilitated.

• The digital world lacks political boundaries. The EU Data Protection Directives concern only the European Member States. Even though Article 25 of the general Directive obliges a Member State to demand equivalent protection for personal data from a country outside the EU, it will have a very limited effect on the hundreds of other countries on the Internet which are out of reach of EU regulations.

In the process of shaping strong and proper personal data protection, an assessment of the inherent risks and benefits of technologies as they emerge is vital.

(48) Google has acquired one of the Web’s most venerated resources, Deja.com’s Usenet Discussion Service in February 2001.
(49) Convention for the Protection of individuals with regard to automatic processing of personal data ETS no.: 108, chap II, Art 5, e. and latter the article 6e of the EU Data Protection Directive.
Long Term Evolution: the Concept of Virtual Identity

The traditional concept of identity is a collection of characteristics which support the identification and authentication process needed in day-to-day social relations and for dealings with governmental and commercial bodies. The usual ingredients are name, civil status, date of birth and nationality, but height, colour of skin or eyes, number of children, educational and professional achievements, etc. can also play a part. Clearly, which characteristics are used at any given time depends on the context and application in question.

The first stage: digital identity

In the Information age, the ‘digitisation’ of identity arose initially from the association of data accumulated by contemporary administrative practice with the memory storage capacity and the processing power of emerging information technologies. This process of digitisation of identity has been going on since the days of the first mainframe computers, and is today an inexorable and irreversible phenomenon.

As indicated in Annex 1 (Evolving User Environment), the use of digital identity and the identification process that goes with it will be at the core of a future environment of ambient intelligence. The citizen will engage in a continuous exchange of data with the networked environment. Without consistent and widely-accepted notions of digital identity and virtual residence, privacy could be exposed to a variety of new threats:

- Extending the span of personal data collected, from today’s passwords, PIN codes and smartcards to tomorrow’s biometrics - fingerprints, voice-print, retina pattern, DNA sequence, etc. These emerging authentication methods may seem at first sight very attractive, but they have dangerous side effects. Biometric keys are considered the ideal solution for authentication because they are bound inextricably to the individual to whom they relate. Nevertheless, unlike other keys, they are not replaceable or transformable (by erasing or upgrading). In case of theft, the damage is irreversible, there is no way back to a safe situation. Consequently, there is an urgent need for research into the reliability of these new methods in view of the proliferation of unregulated initiatives coming onto the market.

- As discussed above, digitisation also provides a unique opportunity to process rapidly, if somewhat blindly, very large amounts of data relevant
to on-line activity. This makes it possible to identify an individual by watching, memorising, cross-analysing and profiling that person’s on-line behaviour. Not only is privacy at risk, but the process generates a perverse feedback effects on the shape of digital identity; the parameters used to define it are constrained by the information systems manipulating the data, and not by any legal framework derived from the needs of the individual and society (50).

- While considered suspiciously by some, anonymity is a basic civil right and one which safeguards privacy and the functioning of democratic society (51). Storing and profiling people’s behaviours on the Internet, or cross-checking individual data with localisation techniques (see above) are examples of how anonymity is strongly prejudiced by the emergence of digital identities.

- Finally, growing digitisation creates opportunities for identity theft because digital records can be duplicated perfectly and leave no immediate evidence of crime. In 1997, Ontario Privacy Commissioner, A. Cavoukian, defined identity theft as the acquisition of key pieces of someone’s identifying information in order to impersonate them and to commit various crimes in that person’s name (52, 53).

Virtual identity

Digitisation has also permitted further development with the creation of virtual identity. Virtual identities were first developed, most visibly, in on-line game activities such as MUD (Multi-user Dungeon or Multi-user Dimension). Since then, driven by various factors such as the explosive growth of social interaction (de MUL, 1996), the increase in human mobility and the introduction of new means of communication, the environment has evolved and virtual identity has acquired a more serious purpose with its own rights and duties. The development of virtual identity will also be hastened by the multiplication of registration processes on the Net. To avoid profiling, individuals will opt for ‘pseudos’ - virtual identities with only the weakest links to real individuals. Additionally, several major companies have entered the business of on-line registration and authentication, and offer users fully

(50) See, for example, TURKLE, 1995.
(51) The usual example refers to the use of real currency, the most generalised and socially acceptable anonymous transactional behaviour.
integrated virtual identities presented as digital "passports" to the cyber-world (preferably the commercial cyber-world): Microsoft’s HailStorm and Novell’s Digitalme are strong examples of controversial offers for digital identities (54). Forums, hacking activities, personal websites (“virtual residences”) and programmable intelligent agents - search engines mainly - further stimulate the development of virtual identities and pseudos. Today, virtual identities can already be borrowed or sold on the web (55). They develop their own curriculum, i.e. in game roles or in queries. They have already progressed to the use of virtual payment systems such as Beenz but could tomorrow be authorised to use credit cards (56). Finally, innovative technologies offer visions of Ubiquitous Computing and Ambient Intelligence worlds where the virtual world is further developed to include multiple human identities and virtual machine identities (57). In this ex-nihilo world, production of multiple identities is the obvious predictable path, linking ubiquitously plural identities into multiple social activities.

Most of existing issues due to the digitisation of identities are relevant for virtual identities. Virtual identities extend this range of issues, offering some new challenges to come.

- Obviously, the identification process, associating one individual to a series of recognisable characteristics, is strongly challenged in the case of virtual identities. Part of their purpose is precisely avoiding any possible correlation. Hacking practices have demonstrated this to the ultimate (58). Identification in interactions and transactions being a matter of identifying responsibility, the emergence of virtual identities and its consequences should be better understood.

- Virtual identities may be considered as a new way for developing privacy-related tools. Hiding behind a pseudo that would have access to the physical world, including to i.e. commercial transactions, is a way of counteracting governmental or companies’ profiling and surveillance.

(54) One of the controversies is about the proprietary aspects of authentication in the Microsoft initiative. However, the very fact of developing and giving a full range of real or virtual characteristics of oneself to such databases is also problematic, calling into question the ethos of companies engaged in these practices.

(55) In 2000, some virtual identities built for game zone were sold on the auction website of Ebay.

(56) http://www.beenz.com/index.xhtml

(57) See i.e. DUCATEL, BOGDANOWICZ, SCAPOLLO, LEIJTEN & BURGELMAN, 2001.

(58) Even if in that specific case, hackers appear to usually leave some digital trace with the aim of being ultimately recognised and acknowledged!
Pseudonymity and anonymity are aspects of growing concern for law enforcement agencies when virtual identity will have determinant feed-back in the real world.

- According to the EU data protection Directive, information is personal if it can be associated with an identifiable individual (59). Virtual identity does not seem to offer that protection: this new way of shaping an identity has more or less no (legal) link with an identifiable "natural" (60) individual. As a consequence, 'virtual individuals' could have no privacy rights. The concept of virtual identity could offer tomorrow a very attractive way of building up huge databases of unlimited detail within the legal framework (CAVOUKIAN & TAPSCOTT, 1996).

- Microsoft and Novell’s initiatives on “Digital passports” have been taken seriously by most commentators, concerned by the trustfulness of such companies when compiling personal data of their clients. Associating an individual to an IP address or a number for a lifetime, in the real- or the cyber-world, necessitates some precautionary thinking.

- Ownership of Virtual identities is a major issue. Considering that virtual identities are, to some extend, pure creations, IPR issues about one’s own personal data, real or invented, are a growing stake.

- More than ever, theft of virtual identities leaves you with no evidence. Possibly not even evidence about the earlier existence of this virtual identity. With no correlation between an individual and a virtual identity, it will be difficult to identify the person who is claiming and the damage that has been generated. Proof is strongly at stake. Further, this threat becomes a major issue for law enforcement regarding the difficulty to collect in a legal way digital evidence of a digital crime or offence.

- Finally, the hacking and modification of virtual identities in a database or at individual level could generate much more confusion than the contemporary forms of hacking. In the absence of reliable correlation between the characteristics of a virtual identity and that of a physical "model", hacking could present irreversible effects.

Virtual identities were first developed, most visibly, in on-line game activities such as MUD (Multi-user Dungeon or Multi-user Dimension). Since then, driven by various factors such as the explosive growth of Internet-based social interaction (De MUL, 1996) the increase in human mobility and the introduction of new means of communication, the environment has

(60) Idem.
evolved and virtual identity has acquired a more serious purpose with its own rights and duties. The development of virtual identity will also be hastened by the multiplication of registration processes required to access services on the world-wide-web. To avoid profiling, individuals will opt for 'pseudos' - virtual identities with only the weakest links to real individuals. Additionally, several major companies have entered the business of on-line registration and authentication, and offer users fully integrated virtual identities presented as digital "passports" to the cyber-world (preferably the commercial cyber-world): Microsoft’s HailStorm and Novell’s Digitalme are strong examples of controversial offers for digital identities (61). Finally, innovative technologies offer visions of Ubiquitous Computing and Ambient Intelligence worlds where the virtual world is further developed to include multiple human identities and virtual machine identities (62).

Forums, hacking activities, personal websites ("virtual residences") and programmable intelligent agents - search engines mainly - further stimulate the development of virtual identities and pseudos. Today, virtual identities can already be borrowed or sold on the web (63). They develop their own curriculum, i.e. in game roles or in queries. They have already progressed to the use of virtual payment systems such as Beenz but could tomorrow be authorised to use credit cards (64). In this ex-nihilo world, production of multiple identities is the obvious next step, linking ubiquitously into multiple social activities.

We can therefore see virtual identity as the next step in the evolution of identity. Virtual identity can be defined as:
- a procedural identity built mainly, if not exclusively, as digital trace;
- having some supports in the physical world but staying largely independent of it;
- created by software to offer personalised services to customers;
- offering the opportunity for multiple identities;
- having the potential to interact strongly with the physical world.

(61) One of the controversies is about the proprietary aspects of authentication in Microsoft’s initiative. But the very fact of developing and giving out to Microsoft databases a full range of real or virtual characteristics of oneself is also a disputable matter and questions companies' ethos.
(62) See i.e. DUCATEL, BOGDANOWICZ, SCAPOLO, LEIJTEN & BURGELMAN, 2001.
(63) In 2000, a couple of virtual identities built for game zone were sold on the auction website of Ebay.
(64) http://www.beenz.com/index.ihtml
According to the EU general Directive, information is personal if it can be associated with an identifiable individual (65). What will happen with virtual identity? This new way of shaping an identity has more or less no (legal) link with an identifiable "natural" individual (66). Should a 'virtual individual' have rights like privacy? It may become difficult for 'little brothers' to collect data by conventional means. If this is the case and 'virtual individuals' are deemed to have no legal rights, then the concept of virtual identity could offer a very attractive way of building up huge databases of definition profiles of unlimited detail within the legal framework.

**Conclusions and Future Policy Implications**

**Conclusions**

This part of the overall article has shown that a comprehensive legal framework for the protection of personal data is in place in the EU, and has suggested that apart from its harmonising effects within the common market, the framework has gone some way to redressing a commercial bias in the international guidelines developed previously, by focusing more closely on the rights of citizens.

The article also highlights the divergence of approaches in different trading blocks and countries, and points to the need for continuing international dialogue aimed at harmonising national approaches and facilitating the cross-border flow of personal data without compromising its integrity. The importance of a successful outcome to such a dialogue in order to avoid harmful effects on international trade was indicated, and the Safe Harbour Agreement with the USA described as one such example.

But the overall impression gained from a reading of the report is one of increasing concern that the current framework will not withstand emerging threats to privacy posed by either by the escalation of some current practices in electronic commerce or the evolution of pervasive information and communications technologies towards an environment of ambient intelligence. These concerns may be set against immediate, medium-term and long-term perspectives:

(66) Idem.
• Regarding the current situation, despite the existence of the legislative framework and the efforts of national and international data protection authorities and bodies, privacy abuses continue on a vast and persistent scale. The report notes the widening gap between the privacy protection and commercial practices exploiting the use of personal data, and suggests that this is due in part to problems of enforcement of the legislation and in part because current legislation does not take sufficient account of the huge growth in on-line information systems and services. Personal data no longer resides in a controlled environment of well-defined monolithic databases, but is increasingly dispersed in networks across organisations and frontiers.

• On the medium-term prospects for change, the report concluded that notwithstanding the undoubted benefits to be derived from the new technologies and services of the Information Society, those same technologies will place at risk the integrity of personal data in the future unless adequate protective measures are taken. The medium-term picture drawn was no more than an extrapolation of current practices, but one which will aggravate both the scale of the problem.

• The long-term picture showed a radical departure from current practice, and demonstrated the weaknesses of today’s legislative approaches in managing future privacy concepts. The study only scratched the surface of the problem, and further research will be needed to enable a better understanding of the implications of virtual identity and nature of the problems that public authorities might be faced with in the future.

**Future policy implications**

There is a clear risk that inadequate security and protection of personal data will alienate citizens and consumers from the systems, services and thus the benefits of the Information Society. In the absence of concrete policy measures, public concern over privacy and its protection will become a serious bottleneck in the future. The challenge facing policy makers therefore will be one of securing the trust and confidence of citizens by ensuring that the right measures are taken.

The first steps in this process are already under way with the current proposal for a revision of the Telecoms Directive (97/66/EC) as part of the
Reform Package now in the stages of adoption (67). The proposed changes include:

- generalising the definition of services by changing the existing reference to "telecommunications services" to "electronic communications services";
- to ensure the protection of a right to privacy on the Internet;
- to separate clearly the regulation of transmission from the regulation of content;
- to adapt and update the existing provisions to new and foreseeable developments in electronic communications services and technologies;
- to create rules which are as far as possible technology-neutral.

However, a broader approach is needed to address the threats to privacy that will emerge over the present decade. The will be different ways of categorising the elements of such an approach; one way is to classify policy measures according to whether they are legislative, self-regulatory or technological in nature.

**Legislative measures**

Identifying a person with the kind of certainty that currently exists in the real world will require adaptation of the existing legal and institutional framework. That framework will need to provide reference points for identification which take account the new parameters and characteristics of identity provided in the virtual world. It would include developing rules for:

- establishing unique identifiers such as life-long IP addresses, generic individual numbering, etc.;
- assessing the reliability of new methods of identification and authentication such as biometrics.

The legal framework would also need to provide adequate privacy protection and safeguards against the aberrant and criminal use of identity. The relevant areas include:

- international consensus on the concepts of identity and personal information in order to avoid the emergence of safe havens for criminal behaviour making use of identity;
- clarification and harmonisation of the use of digital data as evidence in criminal proceedings;
- a definition of the role of, and right to, anonymity in the new context;

- the future trade implications and a reaffirmation of the inviolability and non-negotiability of privacy rights in the face of trade pressures;
- legal clarity on IPR issues relating to personal data at the virtual level.

Specific legislation may be needed in the sensitive area of healthcare data for example:
- the definition of legitimate uses and users of personal health data;
- creation of a user’s duty of confidentiality equivalent to a professional duty of medical secrecy, and establishing user accountability for the data applications;
- ensuring citizens’ rights to oppose the use of their data for secondary purposes.

**Self-regulatory measures**

While many legal experts regard privacy as a constitutional right to be safeguarded by the State, there appears to be an undeniable *de facto* role for self-regulation. The issue to be explored here is whether the application of self-regulation dilutes either the essence of the privacy right or the responsibility of the State to oversee that right. In some countries, the legislation makes provision for the judicial review and supervision of self-regulatory schemes, but this is not the case everywhere.

The clearest area for self-regulation is in standards-setting for privacy practice. The objective here is to create standard procedures which will ensure that through conformance to them, businesses can demonstrate the alignment of their internal practices to the legal requirements. Apart from reassuring customers, adherence to such standards could be a valuable marketing tool for companies through the use of suitable labels and certificates of compliance.

**Technology and areas for further research**

The very strong market driver of personalised e-commerce products and services was described as both a benefit to citizens’ well-being and a threat to their privacy. One way to redress any balance in the market’s favour would be to offset invasive e-commerce practices with the use of suitable privacy-enhancing technologies (PETs). These can provide a measure of privacy protection and can facilitate anonymity and pseudonymity.
Some claim that the use of PETs within a regulatory framework could be interpreted as the State delegating its responsibility for the protection of privacy to the potential victim of a violation of that privacy. These claims regard this effective abrogation of a responsibility to protect one of the fundamental rights of its citizens as a retrograde step in terms of human rights legislation.

Regarding areas for further research, there is a need for risk management exercises to be carried out on emerging Information Society technologies which could be instrumental in promoting criminal abuse, as well as an analysis of the application of the precautionary principle to the use of such technologies.
Bibliography


