Gattiker, U. E., Fahs, R., Blaha, J. & members of EICAR Working Group 1. (March 1998). Medical information and the Internet: Managing disclosure effectively with the help of encryption and privacy. Paper to appear in Proceedings of the European Institute for Computer Anti-Virus Research (EICAR) 1998 Annual Meeting, Munich, Germany.

e i c a r

European Institute for Computer Anti-Virus Research

Published in Proceedings of eicar Annual Conference 98 Munich (Germany)

Working Group 1 (Threats to Information and Property)

Medical Data Disclosure
Encryption and Public Policy as Effective Means for Privacy Protection[1] [2]

Urs E. Gattiker
University of Aalborg, DENMARK

Rainer Fahs
Jaroslav Blaha
NATO Air Command & Control Systems Management Agency (NACMA), Belgium

in collaboration with members of EICAR Working Group 1 -- Threats to Information and Property

E-Mail: EICAR_INFOSEC@bigfoot.com or the Web:http://www.eicar.com/wg1.htm

Preamble: This paper is based in part on the online discussions held using Working Group 1's list server during Winter 97/98 through Spring 98. As such it reflects a joint effort between the moderator (first author), Rainer Fahs, Jaroslav Blaha and other group members who contributed in various formal and less formal ways to the content and shape of this report. This version of the report was written specifically for the EICAR Annual Meeting 1998 held in Munich, March 16 - 18 and has been updated since then. For EICAR INFOSEC -- WG 1 materials pertaining to this topic and related ones, as well as joining EICAR, please check the group's Web site listed above.

Abstract: Rapid cost escalation in health care have forced governments and businesses (e.g., insurance brokers and companies in general) to reduce or at least contain rising health care costs. One viable option has been to improve medical record keeping and its accessibility by parties involved in care taking and administration. Divergent stakeholder demands for information and its privacy may result in conflicts between parties (e.g., insurers versus patients). Encryption technology may help to protect the privacy and confidentiality of patients' information. Unfortunately, governments demanding to be given the possibility of intercepting and monitoring such electronic data transfer for administrative, legal and law enforcement purposes should the need arise is threatening the privacy of patients. This paper reviews these issues and highlights some of the problems and pitfalls various stakeholders are faced with considering medical information, privacy, encryption and law enforcement needs in an international context. Implications for managers and system specialists are provided, and how these issues may affect direct marketing, customer databases and electronic commerce is discussed.

---

[1] Please send comments and requests for reprints to Urs E. Gattiker, Obel Family Foundation Professor of Technology and Innovation Management, Department of Production, Fibigerstraede 16, DK-9220 Aalborg, DENMARK. Telephone:+45 9635-8962 (afternons only); Fax: +45 9815-3030; Home Office: +45 222 111 40 (mornings and evenings); E-Mail: EICAR_INFOSEC@bigfoot.com or for additional information or downloading of this paper please point your browser to: http://www.eicar.com/eicarwg.htm#working_group_1 or also http://www.TIM-Research.com/Papers

[2] The contents of this article to do not in any way reflect opinions of either employer of the three authors. Usual disclaimers apply.

Fiscal restraints and cost cutting by insurers and governments alike has not stopped the rise in health-care costs in North America and Europe. Some suggest that demand for these services will not moderate unless consumers face charges. In turn, these may reduce the escalation of health care-costs, but such charges are unpopular with the public ("Coughing up," 1997). A viable option is a better use of technology which can help in improving the management of delivered care and thus reduce the rapidly rising health care costs. To achieve this goal, information systems storing and processing medical records have become of paramount importance. The latter provides a lot of information about an individual's medical history for doctors and medical specialists. In turn, more appropriate health care can be provided thanks to extensive information available to care givers, while duplication efforts for obtaining data and medical history (e.g., when changing one's general practitioner) are reduced. Moreover, the likelihood for giving inappropriate care due to sketchy information is lowered as well. Finally, prescribing drugs to which a patient might not respond well, or experience undesirable side effects (e.g., nausea), can be reduced by providing the attending physician with a full medical history. In turn, the rapidly escalating costs for prescription drugs could also be managed better.

While medical information may be important to care givers, medical records are also of prime interest to insurers, pharmacists, pharmaceutical firms and medical appliance manufacturers/distributors. These firms can tailor their service and/or marketing efforts better with the help of additional information, while hopefully also reducing their costs. In turn, savings or at least cost containments could be passed on to clients. Naturally, we leave a trail of data behind every time we visit the local health professional. Unfortunately, mischievous intent can always result in such information ending up in the wrong hands. Accordingly, while medical information systems may help in containing the rise in health care costs to some degree, threats to patients' privacy must be carefully considered.

Unfortunately, there have been insufficient research and discussion on issues concerning the development of standards and procedures to protect the privacy of government and business data as well as privacy of consumer information (e.g., data about a person's shopping habits at the local supermarket). While many governments do have standards and procedures for protection of information, they may not necessarily protect an individual's privacy. Moreover, without commonly defining what privacy means for national and international government organizations [e.g., United Nations (UN) and World Trade Organization (WTO)], disagreements and misunderstandings will continue.

When privacy and security matters are addressed in various reports, law enforcement, national security, corporate or consumer issues are usually highlighted (e.g., Szlovits, Doyle, Long, Kohane & Pauker, 1994; The Walsh Report, 1997). All these groups of stakeholders (e.g., expectant and definite stakeholders, such as clients and consumers, see also Table 3) have particular interests in mind when discussing privacy and encryption issues. By addressing any group's needs and claims satisfactorily, another stakeholder's rights are likely to be infringed upon. Thus, a careful balance must be found for all primary and legitimate stakeholders to make medical information records a viable option in our attempts to improve health care systems, while protecting the privacy and security of such data.

Table 1

Key Terms Used in this Paper

Cryptography	Is the science of keeping a message secret.
Encryption	Encoding of message contents thereby hiding the data/information from outsiders, in turn, the encrypted message is called ciphertext.
Decryption	Denotes the process of retrieving the plain text from the ciphertext.
Algorithms	All modern algorithms use a key to control encryption and decryption
Symmetric (or Secret-key)	Uses the same key for encryption & decryption, or the latter key is easily derived from the encryption key
Asymmetric (or Public key)	A different key is used for encrypting and decrypting a message; accordingly, the decrypting key cannot be derived from the encrypting key.
Digital Signatures	Public-key algorithms can be used to generate a digital signature, which is a block of data used to create some secret key.
Public key	The public key is used to verify that the signature was really generated using the corresponding private key. Public keys are often registered with a third party and can be downloaded so the person can check if the key is genuine.
Private key	The party initiating the sending of the document with the signature generated generated this key; it is needed to generate the digital signature.
Privacy	Could be defined as the right of the individual to determine his or her communicative contacts and the right to control the use of personal information by others.
Key Recovery (sometimes called Key Escrow)	Provides some form of access to plain text outside the normal channel of encryption or decryption for a third party such as a law enforcement agency.
Trusted Third Party Encryption (TTPE)	Private keys are either stored with a public or private agency acting in a trust capacity. The existence of a highly sensitive secret key or collection of many keys must be secured for an extended period of time.
Tempest	Transient Electro Magnetic Pulse Emanation Standards which allows a party to do data snooping without the harmed party being aware of its privacy being violated.
Pretty Good Privacy (PGP)	A software package permitting users to use encryption when exchanging messages, widely available. Export versions of PGP are different than versions used in the USA and Canada.
PMI	Provider of medical information; could be a firm doing this job on behalf of the government or a government agency/department providing the service.

Note. When developing this Table we benefited from work by others ("Cryptographic algorithms," not dated*).*

Table 1 outlines some of the terminology used throughout the paper. The purpose of this paper is to:

(1) Discuss both technical and social issues, as far as encryption and privacy of medical records are concerned;

(2) address how various stakeholders' interests can be made more compatible (e.g., governments' requirement for interception and monitoring of electronic data transfer versus patients' demand for privacy);

(3) discuss how these issues may limit our possibilities for reducing health care costs; and,

(4) deliberate some of the practical and research implications.

1. PRIVACY AND ENCRYPTION OF MEDICAL DATA

In this section we discuss the privacy and encryption options available in order to set the stage for the latter part of the paper. Accordingly, the material simply represents an introduction to privacy and encryption (see also Table 1 for definition of terms) which is needed to address these concerns as far as medical records are concerned.

1.1. What is Privacy?

Article 12 of the Universal Declaration of the Human Rights (Privacy International, 1996) states that privacy includes one's right to be left alone. The California Supreme Court further reaffirmed this in a decision in Long Beach City (Doss & Loui, 1995). The right to be left alone provides the individual with explicit self-determination about the selection of interpersonal contacts and, most importantly, contacts between organizations and the individual.

The one international agreement governing privacy issues and principles is a document by the Organisation for Economic Co-operation and Development (OECD, November 1980). These guidelines establish principles for the protection of privacy and trans-border flows of personal data for OECD member countries. Specifically, they govern:

- the collection, use, and disclosure of information relating to individuals by **public and private organizations**; and

- access by each individual to information relating to that individual as held/stored by **public and private organizations**.

Most important are the eight principles of privacy as outlined by the OECD, which are as follows:

- collection limitation
- security safeguards
- data quality
- openness
- purpose specification
- individual participation
- use limitation
- accountability

Privacy is also defined as the right to control personal information (Katsh, 1994). This right can be described as control over data, such as credit information (Culnan, 1993). Linking these two approaches, privacy is defined in Table 1 of this paper. Accordingly, if the individual does have the right to control personal information, does this, in turn, mean that the owner of the information is able to select protection measures or is it left to the discretion of the agency or firm (e.g., health insurance carrier) to decide? Strong encryption mechanisms and protection measures for the control of transient emanations (TEMPEST) are government controlled in many countries (e.g., USA export control, Wassenaar agreement on export controls for conventional arms and dual-use goods and technologies) ("The Wassenaar arrangement," 1995). This means that it is technically and economically unfeasible for the individual and for commercial organizations to control and protect their own private data to an extent that they determine themselves and, as importantly, with measures selected at their own discretion.

The above indicates that some regulatory and legislative efforts have been undertaken. Unfortunately, privacy protection may be hampered by governments using wrongly defined requirements for national security in order to retain capabilities for their intelligence or law enforcement agencies. This could result in actions that may well go beyond legislative parameters and checkpoints. For instance, Swiss media reported that Swiss police had secretly tracked the whereabouts of mobile phone users via the government-owned telephone company. The latter's computer records provided police with information, going back more than half a year, about subscribers' calls, from where and when calls were made, to how long and to whom these calls were made ("Swiss police have secretly", 1997). Worse is that in many people's minds, their legitimate right to access and control their personal information has already been lost. New technologies and large databases facilitate the increasingly effective exploitation of information about consumers and citizens (Schlossberg, 1993).

A massive telecommunications interception network operates within Europe and, according to a new study circulating on the Internet, "targets the telephone, fax and e-mail messages of private citizens, politicians, trade unionists and companies alike." The report says that the network has the ability to tap into almost all international telecommunications as well as parts of domestic phone traffic - and is apparently operated by intelligence agencies without any mechanism of democratic control. The network, dubbed ECHELON, is described in a new study by the European Parliament titled "An Appraisal or technologies of political control." The report was written by Steve Wright, an analyst with the Omega Foundation, a British human rights organization, performing work on behalf of the European Parliament section known as STOA (Scientific and Technology Options Assessment) (Giussani, 1998).

The above suggests that total protection of privacy is impossible, and even taking a violator to court can be difficult and expensive (van Swaay, 1995). Moreover, privacy protection requirements are conflicting with those of governmental organizations, such as law-enforcement agencies and intelligence services wishing to retain the capability to access any information at any time, with no notice to its owner. In addition, invasion of privacy is often also the result of conflicting interests in the commercial world. Direct marketing firms try to exploit personal information about consumers, but the consumer is generally not consulted for agreement and in most cases would prefer to be left alone. To illustrate, if a client calls a restaurant to order dinner for home delivery, the restaurant may obtain the telephone number through Caller Number Identification (CNID). This telephone number may be stored on a database for marketing purposes (for example, to mail flyers with special offers to the client), or the number may be sold to other organizations such as direct marketing firms. Blockbuster Videos was taken to court in 1986 for selling data about clients' movie rental preferences

(Bloom, Milne & Adler, 1994). Another example is USA News & World Report, which was taken to court for selling subscriber information to interested firms (Avrahami, 1996). Often, firms use negative option selling plans, whereby unless a client refuses the service (e.g., selling of address to marketers or providing ad-on services free for a trial period, thereafter charging the customer a fee), it is assumed one wishes to receive it (i.e., silent acceptance). Firms find the use of such techniques beneficial if it is assumed that the majority of customers are unlikely to reject the offer (Spriggs & Nevin, 1996), although negative publicity and/or customer complaints may result in a firm changing its plans (e.g., "The people vs.AOL", 1998). As far as privacy is concerned, some have suggested that it must be implied that the person has chosen to opt out (i.e., not to participate; protect one's privacy), unless one informs the organization otherwise when being asked (see also Section 3.2.2.).

People also differ in how they might feel about certain privacy invasions. For instance, Gattiker, Kelb, Janz, Hosten, Greshake, Schwenteck and Miller (1997) reported that individuals were more concerned about their loss of privacy due to e-mail than to phone calls trying to sell them a product and/or service. Also, people are probably more concerned about unwanted disclosure of their medical and financial data to others, than their preferences about sports or TV-watching habits.

1.1.1. Privacy Protection

Selecting the appropriate protection measures will be a challenge for legislators and organizations/private citizens alike. In most countries, with the exception of Pretty Good Privacy (PGP), strong encryption technology and TEMPEST equipment for private or commercial use (see also Sections below such as 3.3.) is either not available, requires a license or is conditioned on key recovery or escrow schemes (see also Table 1 for explanation of these terms). Probably worse is that by having access to these technologies, agencies are able to bypass existing laws and regulations without the individual or firm being even aware of it having happened. For instance, the privacy protection act in Germany prohibits the random monitoring and wiretapping of individuals. Unfortunately, if the party does not know that data transfer has been intercepted, and there is absolutely no trace of interception of transient emanations for example, the individual cannot use the law to act against such privacy violations.

1.2. Security of Information Systems and Cryptography

The above sections indicate that privacy issues have come to the attention of the media and the public; however, potential conflicts between private citizens', commercial users' and government agencies' interpretation and protection or violation of privacy are numerous. One of the challenges remaining is how to protect privacy while upholding the public's right to and/or freedom of information (e.g., access to data of interest to the public. The increase of information systems and globalization of business further necessitates efforts to protect data not only for confidentiality, but also for integrity and availability. However, systems and data also become increasingly vulnerable to a greater variety of threats, such as unauthorized and unknown access and illegitimate use, alteration, and/or destruction. Proliferation of computers, increased computing power, interconnectivity, decentralization, growth of networks and the number of users, all increase a system's vulnerability. Some have suggested that systems containing more than 1,000,000 people's records should not be built because confidentiality, integrity and availability requirements cannot be met satisfactorily (Andersson, 1996) (cf. Table 1). Moreover, convergence of information and communications technologies and our increased dependence on their daily use makes us more dependent upon such systems. For instance, power outage may result in a pharmacy being unable to

process transactions because its information systems are no longer functioning. A care team may not be able to access a patient's record if the data transfer from a centralized system is interrupted. This could, unfortunately, reduce the quality of care provided by the medical team.

Security of information and communications systems involves the protection of the **confidentiality, integrity and availability** of those systems and the data that is processed, stored or transmitted on them. Table 2 lists these properties and provides explanations. While in theory the three properties are manageable, natural disasters such as the large power outage for areas of Quebec in 1997/1998 (some areas where without power for more than three weeks) show that upholding the properties is often difficult. For instance, diesel generators may work fine for a few hours, but fail to perform at high output for several days, as Quebec's experience shows, thus resulting in data no longer being available or some rural hospitals having to shut down for a period.

Security of Information Systems

Security Issue	Description	Application to Medical Information and Data
1. Confidentiality of Data	Is the property that data or information is not made available or disclosed to unauthorized, parties (e.g., individuals, organizations and processes)	Medical data is not being disclosed to others, such as employers. making the identification of the patient possible.
2. Integrity of Data	Is the property that data and information has not been modified or altered in an unauthorized manner?	Unauthorized personnel are unable to alter medical records while changes made by others are tracked and recorded.
3 Availability of Data	Is the property that data and information, as well as the necessary systems, are all accessible and useable on a timely basis as required to perform various tasks	Medical personnel must get access to patient files even during a massive power outage where generators may have to be used to guarantee availability of data

Note. To improve confidentiality, integrity and availability of data, encryption may have to be used, thereby reducing the information's vulnerability to attacks against its confidentiality and integrity. Naturally, encryption can also help in reducing risks of such attacks in succeeding and compromising medical information (e.g., misuse or alterations). Conceptual and practical suggestions about reducing information systems vulnerabilities and risks can be found in Gattiker and members of EICAR Working Group 1 (1997) (see Tables 3 & 4, Figures 1 & 2).

The relative priority and significance of confidentiality, integrity and availability vary according to the information or communication systems and the ways in which those systems are used. The quality of security for storage and transmission of data with information systems depends not only on hardware, software and other technical measures used, but also on good managerial, organizational and operational procedures (see Gattiker and EICAR WG 1, 1997 for an extensive discussion of these issues).

The growth and commercial development of public networks, such as the Internet, depends on solving the question of trust. As Table 2 suggests, confidentiality of data may be enhanced with cryptography. Data transfer increases risks against data integrity unless cryptography prevents unauthorized parties to alter data when being transmitted from A to B. Hence, cryptography is an important component, helping to make an information and communications system more secure, and ensuring the maintenance of both, confidentiality and integrity of data. However, the widespread use of cryptography raises a number of important issues. Governments, for instance, have wide-ranging responsibilities, several of which are specifically implicated in the use of cryptography. These responsibilities include, but are not limited to:

(1) protecting citizens' right for privacy,
(2) facilitating information and communication systems' security;
(3) supporting economic activities, by, for example, promoting electronic commerce;
(4) maintaining public safety;
(5) raising the necessary revenues to finance their activities; and,
(6) enabling the enforcement of laws and the protection of national security.

Although there are legitimate governmental, commercial and individual needs and uses for cryptography, it may also be used by individuals or entities for illegal activities which can affect public safety, national security, the enforcement of laws, business interests, consumer interests or privacy. Governments and international organizations, together with industry and the general public, are challenged to develop balanced policies to address these issues.

As the above would suggest, the divergent interests which can be affected by either the use or non-use of, or the failure to use cryptography, make the development of balanced cryptography policy both complex and critical. Cryptography, which traditionally has been primarily used by governments, has become widely accessible and affordable to private users in recent years. Moreover, media attention has further raised public awareness about possible benefits and risks with cryptography. This has further increased diffusion of cryptography software being used by many, while the debate about the issues outlined in this paper is continuing.

1.2.1. Secret Key Cryptography

Historically, cryptography has been used to cover secret information from unauthorized parties by encoding. As such, it is important for military and government security. Cryptography uses an algorithm to transform data in order to render it unintelligible to anyone who does not possess certain secret information (the cryptographic "key") necessary for decryption of data. Today, the increased calculation power arising from the development of digital computing makes it possible to use complex mathematical algorithms for encryption of data (Blaze, Diffie, Rivest, Schneier, Shimomura, Thompson & Wiener, 1996).

Secret or symmetric key cryptography uses one common key for the encryption and decryption of information. Although the existing encryption algorithms are very powerful, the drawback of this technique is the administration and distribution of the keys. The same key has to be provided to all communicating parties. Utilizing only one key for multiple parties does not allow for identification of the creator of an encrypted datum (no digital signatures). Also, if the information is modified or leaked, it can not be determined which of the parties possessing the key caused such an incident. The safety of the secret key approach lies in the difficulty to re-engineer the key and the encryption algorithm from the encrypted message. A typical symmetric algorithm is DES (Data Encryption Standard).

The development of information and communications technologies that allow vast quantities of data to be transmitted, copied and stored quickly and easily, has prompted a growing concern for the protection of the confidentiality of data -- including personal data, government administrative records, business and financial information -- and the protection of privacy. Effective and strong cryptography is an essential, if not the only, tool in a network environment for addressing these concerns. Unfortunately, as section 2 suggests, stakeholders' interests and concerns may be detrimental to each other. Accordingly, national defense and law enforcement concerns may be opposite to privacy and security issues of concern to citizens. Furthermore, reports about criminal activity with the help of cryptography have been exaggerated greatly (e.g., Denning & Baugh, 1997). Most importantly, criminals will obtain access to the best cryptography available regardless of defense and law enforcement wishes. Moreover, if similar yardsticks would be applied to telephone conversations and scrambling equipment, defense and law enforcement agencies would have to wiretap all phone conversations. The latter is currently illegal unless a court order has been obtained beforehand. Finally, when asking people whether police should be able to tap into the Internet or whether cryptography should be restricted to help law enforcement, respondents are likely to agree (cf. McClosky & Brill, 1983). Gattiker and Kelley (1998) reported, however, that when subjects are asked specifically to give up part of their own privacy to enable these agencies to monitor their communication, people are very reluctant to do so. Accordingly, why should the measuring sticks for monitoring and limiting the public's ability to encrypt their communication via the Internet be treated differently than standards applied to the telephone? Paranoia may prevent us from approaching this rationally and fairly (cf. Section 2). Besides these issues, there is also some concern about the public key approach as discussed below.

1.2.2. Public and Private Key Cryptography

In the mid-1970's a new development in cryptography introduced the "public "or "asymmetric key" concept, which allows parties to exchange encrypted data without communicating a shared secret key in advance. Rather than sharing one secret key, this new design uses two mathematically related keys for each communicating party: a "public key" that is disclosed to the public and a corresponding "private key", that is kept secret (see also Table 1). The idea of this approach is that it is mathematically easy to generate an associated pair of keys, but that it is almost impossible to determine one key out of the other. This means that the holder of a (sufficiently long) public key is not able to calculate the private key, and thus, for example, fake a digital signature. A typical asymmetric key algorithm is RSA (named after the inventors of the public key approach Rivest, Shamir and Adelmann).

With this technique, if an individual encrypts a message with the public key, the recipient can decrypt it with the corresponding private key. Without the private key, the recipient of the message is unable to retrieve the readable information, thereby reducing the risk of having the information end up with third parties who have no "need-to-know" or of having information being corrupted/altered.

In the above scenario, however, the user has to protect the private key very carefully because once it has ended up in the wrong party's hands, intercepted messages can be decrypted by others without the originator or recipient of the message even being aware of this. Accordingly, public and private key cryptography is only as good as its users' ability to protect their private key. Based on users' sometimes sloppy security of their log-on password, one is allowed to be somewhat skeptical about how much better users will do with their private key.

1.3. Digital Signature

An important application for public key cryptography is the "digital signature", which can be used to verify the integrity of data or the authenticity of the sender of data. In this case, the private key is used to "sign" a message, while the corresponding public key is used to verify a "signed" message. Public key cryptography offers the benefits of confidential transmissions and digital signature in an open network environment in which parties do not know one another in advance. This development allows for broader applications of the cryptographic mechanism, and this -- together with increases in computer power and decreases in computer price -- has moved cryptography into the private sector domain.

Public key cryptography and digital signatures play an important role in developing global information infrastructures. Much of the interest in information and communications networks and technologies centers on their potential to accommodate electronic commerce; however, open networks such as the Internet present significant challenges for making enforceable electronic contracts and secure payments. Several different methods exist to sign documents electronically, varying from very simple methods (e.g., inserting a scanned image of a hand-written signature in a word processing document) to very advanced methods (e.g., using cryptography). According to the European Commission (October 1997), electronic signatures, based on “public key cryptography”, are called digital signatures and are widely considered as crucial for a variety of applications like digital signatures used

- for official communication with public institutions (e.g., calls for tender, exchange of application forms, identity documents, tax declarations, transmission of legal documents),
- for contractual relations in open networks (e.g., electronic commerce and financial transactions),
- only for identifying or authorizing purposes (i.e., in order to be certain of the identity of correspondents or their attributes, such as having the authorization to log into a computer system or accessing a restricted part of a network),
- in closed systems (Intranet),
- for personal purposes.

Naturally, the above applications are rather extensive, and misuse or abuse of the technology is possible. Accordingly, application issues must be addressed and firms as well as governments are still grappling with these issues. Without eliminating potential fears of users concerning secure and safe use of such signatures, their use will be limited as the section below outlines.

1.3.1. Application of Digital Signatures

There is a tremendous potential for fraud in the electronic world. Transactions take place remotely, without the benefit of physical clues that permit identification, thus making impersonation easy. The ability to make perfect copies and undetectable alterations of digitized data complicates the matter. Traditionally hand-written signatures serve to determine the authenticity of an original document. In the electronic world, the concept of an "original" document is problematic, but a digital signature can verify data integrity, and provide authentication and non-repudiation functions to certify the sender of the data. If a document itself has been altered in any way after it has been "signed", the digital signature will so demonstrate. Similarly, once a document is "signed" with a cryptographic key, the

digital signature provides proof that the document was "signed" by the purported author. In turn, the sender cannot easily deny having sent the document or claim that the information has been altered during transmission (cf. OECD, 1997).

1.3.2. Legal Questions with Digital Signatures

The implementation of digital signatures as a cryptographic mechanism to support authentication and non-repudiation security services seems to offer a technical solution to a legal problem. However, it must be mentioned, that there are some legal questions that need to be addressed and, unfortunately, they are addressed differently in various countries. The following aspects are currently being discussed regarding legal concepts behind digital signatures, and requirements on form and procedures:

- Does a digital signature meet legal requirements?
- Is a digitally signed document recognized as evidence in court?
- Does a "Declaration of Intent" have a legal value?
- Are there technical solutions to make sure that users sign a document in the version which is actually visible on their screen?
- Does a digital signature prove that a particular person actually signed a given document?

The last point especially is of some concern because conventionally, a person signs a signature by hand. In the electronic world, however, the technology would permit a third person – authorized or unauthorized – to sign a document, if this person is in possession of the private key ("undisclosed delegation").

Cryptography can also provide technical solutions for the protection of intellectual property in digital form. For example, a digital signature together with a verifiable time-stamp can give authors some control over their work by tying an electronic document to the issuer and ensuring that the document is not modified without detection. The same technology can be applied to ensuring the authenticity and integrity of documents archived electronically (OECD, 1997).

1.3.3. The Need for Action within Europe

The above sections on cryptograph and, especially, digital signatures suggest that countries have to move beyond the basic agreements made under the OECD's umbrella (OECD, 1997). Some member states of the European Union have already proceeded to develop detailed regulations for digital signatures. Germany has released a law on digital signatures (Bundesministerium fuer Bildung, Wissenschaft, Forschung und Technologie, October 8, 1997). France has adopted a new Telecommunications Act (Loi N° 90-1170, 29 December 1997) which is being criticized by various groups, including the French Parliament's Commission for Post & Telecom Public Service (CSSPPT) (Thorel, 18 December 1997). Italy adopted a law on the use of electronic documents and contracts (Council of Ministers, August 5, 1997). The UK government has launched a Public Consultation on the regulation of Trusted Third Party encryption (TTP) [uk_crypt]. The Dutch Government has created an inter-departmental task force [Staatscourant nr. 54, 18.3.97]. Denmark and Belgium are also preparing draft legislation on digital signatures. [http://www.agoraproject.org/]. The Swedish government organized a public hearing in June 1997.

Whilst the development of a clear framework is welcomed, the very divergent legal and technical approaches which have already appeared constitute a challenge. Moreover, the absence of any legal environment in some EU member states – while possibly justified – might constitute a serious barrier for communicating and doing business throughout the EU using digital signatures. This will undermine the free circulation of digital signature related products and services within the EU's domestic market, while hampering the development and expansion of electronic commerce. If e-commerce should be stimulated, then obstacles to digital signatures and free circulation of information must be of highest priority. As well, facilitating the use of digital signatures across national borders requires a common framework at the EU level. Such a framework is urgently needed and should be put in place at the latest by the year 2000 ("Towards a European framework", 1997).

2. STAKEHOLDERS AND MEDICAL DATA DISCLOSURE

Section 1 above discussed privacy issues as far as medical data stored in computer information systems are concerned. In order to improve such a system's confidentiality, integrity and availability, as well as privacy and security, we outlined encryption and digital signature possibilities. As such, while encryption techniques could help in protecting the confidentiality of data and thus not infringe on patients' privacy, the lack of a comprehensive legal framework might make use of encryption more difficult. Also, how digital signatures can be used effectively across national borders or even within countries to assure the authenticity of medical data about a patient in the emergency department is still not clear. In this section we are focusing on medical data and its disclosure to various parties, and how this relates to security and privacy of data, as well as how encryption and digital signatures may help to uphold confidentiality, integrity and availability of medical data as required.

Detailed records on every treatment, drug, and change in condition of a patient provide up-to-date and reliable information. This is essential for making good decisions about health services. At the same time, health authorities and medical personnel need access to such data in order to reduce inadequate or even harmful treatment, while reducing costly duplication and waste of public funds ("Striking the right balance", 1996). There are numerous efforts under way to link patient records nationally and provincially/statewide by various governments such as the USA and the Province of Alberta, Canada (Gostin, Lazzarini & Flaherty, not dated; "Strategic partner selected to develop", 1997). The hope is that with the help of personal identifiers, birth dates and social security/insurance numbers and/or national health numbers, a large information system can be created. In turn, it is hoped that the electronic flow, interchange and use of patient medical records between health care organizations and other parties, such as insurance firms, will be facilitated to save time and costs (e.g., "Sequoia Software chosen", 1997).

But some have argued that such large information systems can hardly meet the criteria in Table 2, while the patient's demand for privacy is nearly impossible to satisfy due to the large number of parties obtaining access to such information (e.g., Anderson, 1996) (cf. Section 3.1.1.). This raises the issue of which stakeholder groups should have access to medical data, the value of information to these stakeholders, and possible conflicts of interest between the various groups of stakeholders. This is discussed in the sections below.

2.1. Stakeholder Groups and Their Divergent Needs for Access to Medical Data

Stakeholder theory (Freeman, 1984; Donaldson & Preston, 1995) and experiences from environmental stakeholder pressure (Ulhøi & Madsen, 1998) suggest that a thoroughly

performed stakeholder analysis can improve the likelihood of optimizing corporate and governmental strategic initiatives. Ulhøi (1997) reports, that organizations agree that the importance of stakeholders for managing will increase, thus satisfying their needs continues to be a paramount issue for managers and policy makers (see also Simon & March, 1958, Chap. 3).

Mitchell, Agle and Wood (1997) suggested that we expand our theoretical concept of stakeholder typology and distinguish stakeholders according to their power, legitimacy and urgency while grouping them into **latent**, **expectant** and **definite stakeholders**. For **latent stakeholders** we can separate along three types. Dormant stakeholders include groups/individuals which have power that remains unused, such as the media which, if necessary, can force the firm or politicians to shift rapidly (e.g., use of human organs from Chinese prisoners being used for transplants resulting in negative publicity world-wide in 1997). Discretionary stakeholders may be soup kitchens receiving contributions and free samples of over-the-counter pain killers from drug companies, while demanding stakeholders could be the lonely demonstrator in front of government offices.

Mitchell, Agle and Wood (1997) also suggest that **expectant stakeholders** are made up of dominant stakeholders (e.g., large institutional investors, employees, key customers), dangerous stakeholders (e.g., wildcat strikers, terrorists) and dependent stakeholders (e.g., public demanding that a firm reduces pollution may unite with media or government to get action). In the latter case, the public might demand legislation preventing insurers from getting access to data from genetic tests which could indicate how prone a person might be to develop a form of cancer later in life. An example might be an insurance company, which could have purchased information illegally from data administrators of cancer clinics enabling it to more accurately determine clients' health status. In turn, such information would help the insurer to adjust premiums accordingly.

Table 3

Stakeholder Typology: A Framework for Medical Information

Typology of Stakeholders	Description	Application to Medical Information and Data
1. **Latent akeholders**	Have usually one attribute, i.e., power, legitimacy or urgency. Little attention by management since this group is likely to take a passive stance toward the provider of medical information (PMI)	
1.1. Dormant stakeholders	Have power to impose will on firm but may lack legitimate relationship or urgency to do anything	Media writing a story about how medical records are being used.
1.2. Demanding stakeholders	The sole relevant attribute is urgency, such as a sole	Sole citizen who demands the Privacy Commissioner or

	demonstrator calling for a particular action	ombudsperson do something.
1.3. Discretionary stakeholders	Have the legitimacy attribute but no power nor urgent claims on the organization, such as the cancer foundation obtaining funds and voluntary labor from the PMI or a medical insurer	May receive help with having their database about donors and/or members put together by an employee volunteering time and know-how.
2. **Expectant Stakeholders**	Two attributes, power, legitimacy and/or urgency are present; have an active stance, and thus PMI is more responsive to expectant stakeholder than to latent one	
2.1. Dominant stakeholders	Legitimate claims and power because can act on them. such as investors, employees, key regulators and suppliers	This group may demand special procedures; for instance, regulators outlining how a citizen can get access to one's records.
2.2. Dependent stakeholders	Urgent legitimate claims but need ally to be heard such as small shareholders and/or public demanding some action	Consumer advocacy groups demanding better privacy policies for the health insurer collecting and using of patient information.
2.3. Dangerous stakeholders	Have urgency and power but no legitimate claims such as the Unabomber (or terrorists) being charged in 1996 in the USA	Hackers and spammers who may use various means to unlawfully gain access to medical information records subsequently being used for their own needs and/or requirements.
3. **Definite stakeholders**	Have power and legitimacy, additionally, their claim is urgent, such as government health agency requiring information in case of epidemic from PMI. Its demands may be given priority by management	Key suppliers, such as doctors, demanding immediate attention (e.g., need for complete medical history on an insured patient to help fight deadly virus discovered in a patient's blood).

Note. Part of the above Table is derived from Mitchell, Agle and Wood (1997), while extensive additions have been made to make the stakeholder identification and salience applicable to medical databases.

PMI = Provider of medical information which could be a firm doing this job on behalf of the government or an agency/department of the latter.

As Table 1 illustrates, the final overall group is made up of **definite stakeholders**. They have power and legitimacy already; hence, a major customer may force a firm to change behavior (e.g., pricing policy). While in Table 3 we primarily see stakeholders as interest groups which can take advantage of their power and legitimacy depending upon the urgency of their concern, Ulhøi (1997) argued that a company may not perceive its configuration of stakeholders only in terms of threats. Instead, the firm may see some of its stakeholders from an opportunity perspective, such as learning from their needs, expectations, and expertise.

Table 3 above illustrates the typology used for stakeholders. We are primarily interested in **expectant** and **definite** stakeholders; nevertheless, any viable information technology strategy requires that **latent stakeholders** (e.g., media, government regulators from other countries) are considered as well. Any party accessing medical records (aggregate statistics/data and/or data with individual identifiers) represents certain interests. Moreover, the value of such information to various stakeholders (e.g., insurer and individual) necessitates that the appropriate encryption and privacy strategies must be implemented with the help of feasible techniques (e.g., encryption and digital signatures). Finally, a latent stakeholder may become an expectant, if not dominant, stakeholder depending upon circumstances. For instance, patients infected by the AIDS virus through contaminated blood given with transfusions may first be latent stakeholders for the firm that collected the blood. The latter provided it to the hospital, which, in turn, was giving the patient the transfusion during surgery. However, if the virus is detected, as experiences in France showed, latent stakeholders may become expectant ones, and demanding one at that (e.g., demanding punishment of government health officials, as well as suing various doctors, hospitals and organizations supplying and using blood contaminated with the Aids virus).

2.2. Information Content

As the above suggests (see also Table 3), expectant and definite stakeholders, as well as latent ones, may have divergent and often conflicting interests. These must be balanced against each other to avoid conflicts and privacy violations. Patients are a general practitioner's expectant stakeholders and dominant at that. For the patient, the doctor-patient privilege is probably sacred. Hence, the doctor is as much interested in keeping a patient's health record private as the latter since the patient may complain and possibly sue the doctor if he or she fails to use the necessary safety and security procedures to protect health record confidentiality, integrity and availability. However, neither doctor nor patient are sharing the information alone. Instead, information about prescriptions for drugs, treatments and referrals are all digitally stored and used by various parties (e.g., pharmacist, insurance company or government, if national health care program for payment). The likelihood that information will be improperly disclosed depends on three things as outlined in Table 4.

Table 4

Factors Influencing the Likelihood of Information Being Disclosed to Various Stakeholders

---

1) ***its value*** (e.g., to the insurer, employer and patient)

2) ***the number of stakeholders and people who have access to the information****, and*

3) ***legitimate versus illegitimate access to information*** by stakeholders and others.

Note. The above factors increase the threat against maintaining database confidentiality, integrity and availability at all times (see Table 2).

Stakeholders can obtain legitimate or illegitimate access to medical data (cf. Table 4). In computer security models, people are considered to be intangible assets, whereby their motivation and capabilities must be considered as well. Accordingly, regardless of the value of information and how many stakeholders get access to it, the number of illegitimate accesses must be reduced to an acceptable minimum. Most importantly, users must be motivated and skilled enough to follow procedures and apply offered security techniques vigorously, thereby reducing the availability of data to unauthorized users while upholding confidentiality and integrity as much as possible (cf. Table 2).

The greater the detail about a patient's every treatment, drug, change in condition and medical history back to birth in a database, the more reliable such information will be for health care providers. While the value of such information to one's physician for making better decisions about health services is high, other stakeholders might also consider such information to be valuable and thus demand access. At the same time, health authorities and medical personnel elsewhere might need access to such data as well, in order to reduce inadequate or even harmful treatment, while reducing costly duplication and waste of public funds (e.g., No Author, December 5, 1996). Accordingly, the dilemma is that the more complete the database, the greater the number of people and agencies requiring access. In turn, the threat to privacy for patients is increased whenever the number of stakeholders and people (absolute number) wanting access to the data increases.

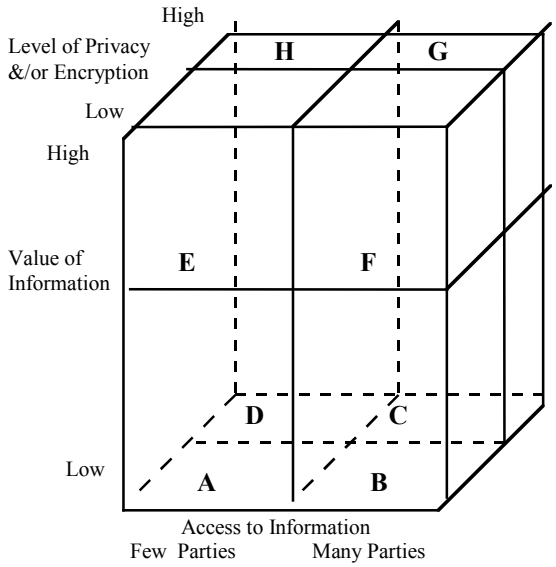

Figure 1. A model for classifying challenges against encryption of medical data and its privacy and safety/security

Figure 1 illustrates this dilemma graphically. Privacy is especially important when many parties obtain access to medical information such as patient records, while the value of such

information for their work is high (see Table 5). Which Quadrant might fit a situation best is also affected by the factors outlined in Table 5. Even using encryption is of limited help if too many unauthorized parties see the information on a terminal or desk when it is decrypted (e.g., print out).

Table 5

Factors Facilitating Efforts for Maintaining Confidentiality, Integrity and Availability of Medical Data

The challenge is to strive for:

1) complete and accurate information in the medical database, which is of substantial value to various stakeholder groups, while in turn

2) limiting the number of people getting access and, most importantly,

3) assuring privacy by using encryption and other methods to prevent unauthorized parties from getting access to medical data files kept in an information system.

Note. The above factors are in apparent conflict because the greater the completeness and accuracy of the data-base. As more groups and individuals want access (Point 2), the greater the difficulty to maintain privacy.

Before further discussing Figure 1, we should point out that, in the end, it must be the patient who determines which medical information the team providing care gets access to. Moreover, the patient must be given the opportunity to object or request that the complete medical record, or parts thereof, is restricted to one or more named clinicians. Accordingly, any large medical database being accessed by public agencies, insurers and clinicians is unlikely to have complete data if the patient has any say. For instance, the person may not want his or her medical records from prison (e.g., indicating extensive psychological counseling helping patient deal with depression symptoms) to become part of the database. The record may contain discrete flags indicating to clinicians and others that part of the patient's medical history is hidden, and lead a clinician to ask the patient if he or she has omitted any information which might be important. Naturally, a health insurance company may misinterpret discrete flags indicating missing information.

Limiting access for various stakeholders either outright (e.g., insurers only get data without personal identifiers) or partially (e.g., flags indicating to clinicians, but not others, that some data are missing due to patient's request) will result in extensive lobbying efforts to change

such laws. Excluded groups or those with limited access (e.g., insurers) will want to obtain unrestricted access primarily on the basis of improving service while reducing costs which, in turn, would benefit patients. Here, the majority of patients who do not have records which might affect their quality of life (e.g., carrying no dangerous disease) might also pressure governments to open access in order to permit them to reap cost saving benefits with lower premiums. Democracy might have to protect minorities from being harmed and treated unfairly. Moreover, confidentiality of medical data is also threatened by the fact that about 10 percent of general practitioners have already experienced computer theft and thus lost patient files stored on the machine's hard-drive (Pitchford & Kay, 1995). Below we describe how the Quadrants in Figure 1 represent the various challenges faced by regulators and managers alike when trying to establish medical record systems of various sizes and depth of content.

2.2.1. Managing Access and Content: Privacy and Encryption Issues

Figure 1 assumes that a high level of privacy is consistent with high levels of encryption used, that is, neither one is independent of the other. Quadrant A in Figure 1 describes a situation whereby an individual's records for over-the-counter drugs purchased at his or her preferred pharmacy may be recorded. The value of the information may be limited except for marketing purposes, while access to it may be given only to the pharmacist using his or her database. Nevertheless, since security measures are not necessarily in place (e.g., data in database is not encrypted), privacy for clients may be low as well, since all pharmacy employees will have access to the patient's file. Transferring files between pharmacies (e.g., in case of a national organization) is likely done without using encryption.

Quadrant B may describe a situation whereby many people get access to a patient's general insurance record (e.g., information about type of insurance). The value of such information is again limited, except maybe for marketing purposes. Moreover, privacy of this information may also be low as it is unlikely that such information is submitted to any encryption mechanisms when being transferred between offices.

Quadrant C might be illustrated by a situation whereby the database provides information about gender and age of subjects; however, personal identifiers are not given for such records while the value of the information is limited except for research purposes. While many people might get access, files may, nevertheless, be transferred in encrypted form only.

Quadrant D may be the general practitioner's private database to which only he or she has access (limited access). The data's value may be limited because no data is available for the time before becoming a doctor's patient and after having chosen another doctor. Incomplete data about the person's medical life history as well as limited access (e.g., doctor and assistant only) do not, however, result in high privacy unless encryption is used.

Quadrant E could be illustrated by a situation whereby data about genetic test results as performed on various risk groups are being collected. In turn, information may provide insights about the person's likelihood of catching a certain disease (e.g., risk for breast cancer). Here it might be possible that a few health professionals have access to such data to assess the potential for exposure to such a disease and effects upon future generations. The information contains personal identifiers for each citizen's record. Here privacy is limited to enable health professionals to do their work, but encryption may also be weak. Once a person has gained access, all information is available since no encryption is used.

Quadrant F could be a patient's medical record, which can be accessed by the attending physician, emergency doctors and the hospital's accounting office (for billing purposes). Privacy is limited since these records must be accessible to any doctor providing emergency care in another state/province to the patient. The value of such information is great to the stakeholders getting access.

Quadrant G represents the ideal but **unrealistic** case whereby medical data is accessed by many, the value of the information is high but, most importantly, privacy is also high. Moreover, the use of sophisticated encryption mechanisms further reduces threats against privacy. For instance, this could be illustrated by aggregate medical data being used for research purposes, whereby privacy is protected by not providing a personal identifier to stakeholders gaining access to such data (e.g., government agencies and medical researchers). Moreover, data may only be stored in encrypted form, thereby limiting its usefulness unless the person has the appropriate key to decipher the data.

Quadrant H again illustrates an **unrealistic** scenario because if a patient's medical history is given in full from birth up to this date, political pressure will be very high for access by excluded stakeholders (e.g., insurers and hospital billing departments). It is likely that, ultimately, besides one's general practitioner, many of these lobbying stakeholder groups will be obtaining access. Such a comprehensive medical database providing a complete medical history of each person is of great value to many stakeholders (e.g., insurer, doctor, government and employer). One would hope that access is limited, while privacy is high, and sophisticated encryption techniques further limit the misuse of such data.

The above information does not try to be complete, but instead provides the reader with an overview of the type of medical record being accessed by various stakeholders. Here Figure 1 implies that high levels of privacy go in tandem with appropriate levels of encryption, that is, without the latter, privacy cannot be safeguarded. In summary, Figure 1 suggests that it is extremely difficult to maintain high levels of privacy if the value of information is high, as is the case with a patient's complete medical history (e.g., Quadrants H and G) (see also Table 4). In such a case pressure becomes great to provide access for many stakeholders. and it will be difficult for the patient to restrict access to a few or keep certain information hidden. For instance, what can an individual do if the insurer refuses to provide life insurance if the firm does not get access to the complete file? Even if such access is restricted (e.g., as per patient's request or by law), applicants may be asked informally to provide a print out of the complete record to which they should have access themselves under any freedom of information regulation. Also, how will an individual be able to prove that data from genetic tests may have resulted in one not being hired or insured? Hence the challenges outlined in Table 5 are nearly impossible to balance to every stakeholder's satisfaction. Below we will address in more detail the privacy issue as it pertains to medical or other records, especially as far as regulation is concerned.

3. SAFEGUARDING PRIVACY: ACCESS AND REGULATORY ISSUES

Any new medical information system containing centralized records from patients has to address the value and access issue as outlined in the previous section of this paper. Since information in such a database is valuable to many parties including the patient, access, encryption, digital signature and privacy issues are of paramount importance. Figure 1 suggests that a careful balancing act between stakeholder interests and needs for information from governments, insurers, employers, doctors, hospitals, pharmacists and,

most importantly, patients is required to succeed as far as privacy is concerned. In turn, while the need for privacy protection of patients' records is needed, data encryption may be required to attain satisfactory privacy levels. Nevertheless, even encryption does not prevent some clever individuals or machines from breaking the code and thus deciphering data or simply stealing such data while violating somebody's privacy (Abelson et al., 1997; Blaze et al., 1997). Below we discuss these issues in some more detail.

3.1. Access to and Value of Information

Table 2 outlined how the security of an information system requires that the confidentiality, integrity and availability of data can be maintained. Table 3 summarized the various stakeholder groups we must deal with when looking at medical information systems such as latent, expectant and definite stakeholders. Figure 1 graphically illustrated what data access and its value might mean for a patient's privacy, and how encryption might be applied effectively to support the former. Tables 4 and 5 outlined some of the factors possibly threatening our efforts to maintain privacy, confidentiality, integrity and availability of data; options we have to reduce threats and vulnerabilities of databases holding important medical information were also sketched out.

While Figure 1 did not address the legitimate or illegitimate use of data, it illustrated graphically how difficult it is to balance access and value of information while using encryption in order to strengthen privacy satisfactorily. At this stage, most efforts for medical databases sponsored by governments indicate that the latter intend to collect as much data as they can in order to facilitate the use of accurate and complete information by health care professionals (e.g.,"Government introduces draft legislation", 1997). However, the greater the completeness of such records, the greater the value of the information they contain to various stakeholder groups. Accordingly, the potential threat by parties wanting illegitimate access increases. Moreover, the threat to confidentiality, integrity and availability of data stored and maintained with such a system -- containing information about several millions of users -- is substantial (e.g., through natural disasters).

Whilst access to such information can in theory be limited to physicians, numerous other people will get access. For instance, in an emergency ward nurses and even orderlies may obtain access to vital information to save somebody's life by using their personal password to speed up health care services provided to the patient.

Naturally, strong identification and authentication measures can be used. For instance, biometrics such as touch pad (for checking genetic fingerprints), language, body's low current and so on may all help in forcing people to access the data personally, instead of "authorizing" somebody else to do so on their behalf. But still, in an emergency the doctor may provide the biometrics information needed to gain access to the database. However, subsequently, the attending physician might be asking the attending resident to search the database and obtain the information required, while the doctor is taking care of the patient at the same time (i.e., division of labor).

It should be made clear that the above described scenario is a description of a "day-in day-out" situation, and that the implementation of a verified security policy based on a solid theoretical mode would not permit such a situation to occur. The problem is the difference between theory and practice where, under certain emergency situations, people resort to measures helping them accomplish their job objectives more quickly, while endangering the confidentiality, integrity and availability of a database and possibly violating a patient's privacy. Here, attribution of record access (e.g., who, when, what and where/location) may not be very helpful as audit trail in trying to close a leak. For instance, 12 people may have

looked at a print out of the file, and the janitor may have collected it from the trash and sold it to an interested illegitimate party. Many more such scenarios can be imagined and are possible. In real life, 100 percent accuracy rates are just theoretical and nearly impossible to achieve.

The above illustrates that biometrics might, in theory at least, help in restricting access to very valuable medical information to parties which really require such information to provide patients with effective and cost efficient health care. Unfortunately, in practice, factors may undermine the use of biometrics and its effectiveness. Additionally, this method may be cumbersome and costly to administer (e.g., keeping biomedical data records for rapid on-line verification around the country). Moreover, some parties may misuse their well-intended privilege for getting access to data by passing information on to other interested but unauthorized parties (e.g., names of HIV patients). Again, technology is only as good as the humans taking advantage of it; this applies to medical information and its disclosure from a database as well.

3.1.1. Using Health Cards: Problems Remain

In Germany, by law, all persons insured in the mandatory public health insurance system are provided with a chipcard containing their insurance data. For now the card contains only administrative data, like the person's name, gender and insurance number. For instance, in Denmark the card number is made up of the person's birth date. One idea is to also store medical data on this card. In turn, this would improve transportability of these data between various health care institutions. The privacy risk is obvious. Encryption could support privacy, for example, by creating three data domains on the card:

1. Public: This domain contains administrative data about the person, as it is already nowadays available. No or only very weak encryption (basically to ensure integrity) is needed.

2. Private: This domain should contain more or less the subject's full medical records (probably including hyperlinks to centralized databases containing X-ray pictures etc.). This domain needs strong encryption and a password system, which allows only access by the patient (Read-only), and a trusted medical party (e.g. personal physician) who can add data and updates. For these updates the combination of the patient's and the personal physician's key would be required, thus providing for traceability of changes.

3. Emergency: This domain contains data readable by emergency and medical services using a general key to access such data. This domain would only contain limited data such as a person's diabetes, cardiac problems, blood group and allergies against drugs. For data updates the same provisions as for the private domain would apply.

The above example would reduce some of the threats inherent in any huge database with records at least at first glance. Nevertheless, to assure integrity and availability of such information, backup procedures would be needed. For instance, if the individual looses the card or it somehow becomes damaged, a centralized database would have to be used to re-issue a card. Hence, the usual threats and risks against confidentiality, integrity and availability of data apply to this centralized database (cf. Andersen, 1996). Moreover, various stakeholder groups will continue pressuring legislators to get access to the information on the patient's health card (e.g., insurer requires annual updates).

The above illustrates that while the German approach, as well as Denmark's if pursued further, might reduce threats to privacy of patient data, in the long term the challenges will be

the same as for a centralized data-base as those considered in the USA, UK and some provinces in Canada.

3.2. Legislation and Privacy

Safeguarding of privacy does in part depend on who gets access, and the value attached, to the information. Accordingly, as pointed out before, the more people have access to information and the more valuable it is for various stakeholders, the more likely certain parties will be to offer a reward for purchasing such information illegitimately (see also Figure 1). Governments have been trying to respond to this challenge by undertaking legislative efforts in national and international forums to further protect privacy. Moreover, while geographical boundaries are removed with new information technology, governments are just starting to grapple with legal and other issues (see also Section 1.3.3. The Need for Action within Europe).

3.2.1. Regulation and Sharing of Data

Many governments are trying to create national or regional databases with their citizens' health care records (e.g., Alberta, Canada and the USA Federal Government for Medicare). The attempts undertaken by the Province of Alberta in Canada to create a province-wide medical database will increase the information available to health-care professionals in the Province. It might even possibly help in lowering costs for health care delivery. However, how data exchange between provinces/states and countries may by handled by the proposed health information system is not addressed in any publicly available document. It must be mentioned here, that such a central database would be the focal point of threat and thus increase the associated risks substantially (e.g., No author, June 11 and July 14, 1997). Accordingly, would Alberta be able to share its data about one of its citizens with another province's health information system in the case of a person moving to or from another province? What about sharing data with the federal government, with or without personal identifiers, for health care policy measure purposes? How would privacy concerns be regulated if access to data were given to parties subject to different privacy legislation (e.g., in two provinces/states)? What about one of its citizens having an accident in the USA or Europe and getting treatment there? Would physicians located abroad get access to such information and if so, how? How will treatment information from abroad be added to the database to assure its completeness? For instance, USA or European laws may prevent a physician providing information about treatment given to an Albertan to a database in Canada.

Besides the challenges for governments as far as legislation and the use of health information by agencies in different provinces/states are concerned, insurance companies providing health care or supplemental health insurance (e.g., for prescription drugs) may demand access to such a database in order to offer lower rates. If such a firm obtains access (partial or complete), can or should it be prevented from using this information when offering life, car and theft insurance to clients? For instance, information from a person's medical data-file can legitimately or illegitimately be used when considering an individual for car insurance (e.g., person receives drug against seizure, should rate be adjusted accordingly?).

Legislation may prevent a firm from using health information from one of its clients for other purposes (e.g., when applying for another insurance). However, insurance firms will lobby against such legislation with the argument that. by being prevented from using a fully integrated database for each customer, huge cost savings cannot be realized. Not having a fully integrated customer data base will increase privacy for clients while reducing the threat against confidentiality of their medical data. Unfortunately, as this example shows, privacy

does not come for free. More privacy means less integrated medical and customer databases with limited access to those only as stipulated by the individual. In turn, cost savings for governments and firms will be limited. Unless some legislation is put into force, privacy protection becomes a financial issue; that is, individuals with the necessary wealth will be able to afford higher insurance rates due to not providing medical records to insurance firms.

3.2.2. Legislation for Public and Private Data

Another problem with a publicly sponsored medical information system is that legislation for public servants and employees from private organizations may differ as far as privacy of medical information is concerned. For instance, Québec has had privacy protection for quite some time on how public organizations were supposed to handle data from and about citizens. In contrast, how private firms are supposed to protect customers' privacy was not really addressed until a bill was put into force in 1993 (Bill 68 1993, Chap. 17; August 4, 1993). Often we have a privacy law for public but not private data, that is, while privacy policies may apply to public agencies, business' and others' use of data may experience limited if any regulation in some countries. Moreover, medical data and privacy have been addressed, but it is not always obvious how general privacy laws for governments and/or private business apply to medical data (e.g., HIV information). Here a firm or doctor may experience a dilemma in cases where one might serve several masters. For instance, the doctor–patient privilege might be threatened if a test is requested on a prospective employer's request. While the HIV data may not be accessible normally, the personal physician may know about this. Can the physician invoke the doctor--patient privilege and thus not report this information to the prospective employer who is paying for the medical tests and the report? Moreover, what will the employer do with such a report and its information (e.g., will it be destroyed immediately or put into the new employee's personnel file) (see also Information Policy Committee, April 1997 for an extensive discussion of this issue)?

As outlined in Section 1.1.1., freedom of information is also an important issue here. For instance, is the individual given permission to restrict access to one's medical file by a government agency (e.g., police) for other uses? To illustrate, at a speed checkpoint police may appreciate having access to a driver's medical data file about his or her possible addiction to a substance and medical or psychiatric treatment against it. In contrast the individual may not want the agency to have this information available when erratic driving due to a small seizure leads to an accident. Today, most countries do not provide an individual with access to police files to check for accuracy of the information. If one has a suspicion, a data privacy commissioner may examine the files on the citizen's behalf. A taxpayer may also claim a deduction for medical expenses when doing annual filing for taxes. In turn, tax authorities might wish to check such a claim against one's medical file, thereby reducing possible fraud and the costs to determine legitimacy of such deductions. Should this be possible and if not, how can the individual check or protect his or her right? Today, most countries only provide citizens with limited recourse against various government agencies exchanging data and collaborating for performing their tasks more efficiently. In turn, the number of people getting access is raised substantially, while keeping data confidential is further reduced. Privacy may be impossible to maintain at a satisfactory level unless huge databases with extensive individual records are not created (see Table 5).

3.2.3. National and International Issues

As the above suggests, even as far as domestic regulations are concerned, not everything is rosy. Additionally, large organizations doing business in the medical/health care field, as well

as in other areas will face a difficult challenge and possibly dilemma trying to satisfy privacy and business demands when using medical databases. In addition, globalization of trade puts another twist on privacy issues for business and governments.

The Québec law (Bill 68) was this province's response to European Union (EU) legislative efforts and regulations first released to the public in 1991 (Directive of the European Parliament and the Council, adopted by the Council July 24, 1995). The EU directive forces member states to adjust their national privacy legislation to meet EU regulations by October 1998. Countries such as Holland and Sweden have already adjusted their national legislation to meet EU regulations, while others such as Germany and Italy are in the process of doing so. After the October 1, 1998 deadline has passed however, EU privacy regulation will affect data transfer and information exchange between organizations in the EU and others outside its borders. Hence, Québec wanted to make sure that its legislation would enable Québec firms to receive and exchange customer and other data with subsidiaries and other firms located in the EU. Many firms located in Ontario have adjusted to meet Québec guidelines and, in turn, most firms doing business across provincial borders in Canada follow Québec 's Bill 68 when dealing with data privacy.

The above illustrates that while official negotiations for harmonization between privacy legislation in Canada and the EU may have been lacking, Québec's efforts have resulted in some informal harmonization between Canada and the EU by bringing Canadian and EU legislation in line with each other. The biggest obstacle for Canada and the EU is how data exchange will be affected after October 1998. But it would be reasonable to assume that a legitimate transfer or exchange of medical information from a database in the EU to the USA or Canada by an insurance firm would not be possible because the latter two's privacy legislations do not meet EU standards. In turn, large insurance companies wanting to outsource their data entry and processing work and/or centralizing their databases to achieve cost reductions and raise efficiency will experience some difficulty in doing so. Here, trans-national negotiations resulting in further harmonization of domestic laws with international ones will be needed to permit firms to centralize their databases with customer and other important data.

3.3. Regulation of Encryption

As the above shows, data legislation for private organizations in addition to public ones still needs effort in most countries, provinces and states. Worse, however, is that even though globalization is becoming ever more prevalent in most business sectors, harmonization of privacy and security laws is lacking. In contrast, an international organization handles disputes quite successfully for trade (e.g., World Trade Organisation = WTO).

As outlined in Section 1 and Table 2, confidentiality and integrity of data are facilitated if encryption technology is applied, thus increasing privacy of data being exchanged legitimately between two parties (cf. Figure 1). In this section we will discuss how encryption policies and legislation may facilitate or hinder organizations' efforts in protecting privacy of their client data.

3.3.1. Export Control Measures

Concerns over foreign threats to national security have been the primary motive for export controls. Whilst countries want to protect their own military and diplomatic communication through encryption, the objective of export control is precisely to deny similar benefits of cryptography to foreign opponents, in particular if they do not have equivalent technical

means. Therefore, export controls are in general designed to prevent international proliferation of certain encryption technologies.

Under the *Wassenaar arrangement on export controls for conventional arms and dual-use goods and technologies* ("The Wassenaar arrangement", 1995), replacing the Co-ordinating Committee for Multilateral Export Controls (COCOM), a group of 28 countries applies export controls to encryption products.

Within the European Union, the *Dual-Use Regulation* (December 1994) establishes a common framework for exports of dual-use goods (Council Regulation (EC) 3381/94, December 19, 1994). This regulation sets up a community regime for the control of exports of dual-use goods (i.e., civil and defense applications) by establishing a list of goods covered by the regulation. Accordingly, certain encryption products may only be exported on the basis of an authorization. In order to establish an internal market for dual-use goods, such export authorizations are valid throughout the EU.

Moreover, according to Article 19 of this Dual-Use Regulation (Council Regulation (EC) 3381/94, December 19, 1994), member states exercise a license procedure for a transitional period and for intra-community trade of certain particularly sensitive products. For the time being, this also includes encryption products. This means the Regulation obliges member states to impose not only export controls (i.e., controls on goods leaving Community territory) on dual-use goods, but also intra-community controls on cryptography products shipped from one member state to another.

The Dual Use Regulation (Council Regulation (EC) 3381/94, December 19, 1994), however, does not fully specify the scope, content and implementation practices of national controls. Consequently, a large variety of domestic licensing schemes and practices exists. Divergence between domestic and EU regulations as well as others can lead to distortion of competition.

3.3.2. Domestic Control Measures

Law enforcement authorities and national security agencies are concerned that widespread use of encrypted communication will diminish their capacity to fight against crime or prevent criminal and terrorist activities. For this reason, in several EU member states, consideration is being given to how their encryption policy could develop in the future. This has led to national and international discussions about the need, technical possibilities, effectiveness, proportionality and privacy implications of such a regulation.

3.3.3. Existing Regulation within the European Union and the OECD

Whilst export control measures are internationally widely applied, up to now, domestic control of encryption is quite exceptional. In fact, currently only one member state of the European Union (France) applies a comprehensive cryptographic regulation. The Prime Minister (in practice the SCSSI which stands for Service Central de la Sécurité des Systèmes d'Information) submits provision, export and use of cryptography to a simple declaration that the cryptography can have no other object than authenticating parties or ensuring the integrity of information, otherwise it must have prior authorization. This law is currently being modified (Loi N° 90-1170, 29 December 1997). Although there have been discussions in other member states, only the United Kingdom has so far launched a Public Consultation on the regulation of TTPs for the provision of encryption services (but not for use of encryption (DTI, 1997)).

The international picture is quite similar. Looking at the OECD countries, besides export controls, there are basically no domestic regulations implemented. In the USA - where up to now no domestic regulation is in place - there is an intensive debate on several legislative initiatives. In taking up the developing debate on this topic in some OECD member countries and trying to avoid obstacles to international trade and commerce resulting from divergent national policies, the OECD has adopted guidelines for a cryptography policy.

3.3.4. Regulation about Use of Encryption

Regulation of use would mean to rule the use of encryption without an authorization as illegal. Alternatively or additionally, supply and import of encryption products and services could be brought under an authorization scheme. Authorizations would either be denied or granted under certain conditions, for instance, to use only weak encryption or to sell only approved software. These conditions are scaleable to satisfy any perceived needs of law enforcement and national security agencies.

Such regulations could limit the use of encryption. In addition, divergence between regulatory schemes might result in obstacles to the functioning of the Internal Market, in particular for free circulation. If an encryption software company, which can freely develop its products in its home country, must comply with specific technical or legal requirements in other member states, this company has to produce at least two, if not more, different versions of its encryption software. The same situation occurs if enterprises want to offer cross-border encryption services.

Today, nobody can be totally prevented from encrypting data (criminals or terrorists can use encryption for their activities) for three reasons:

1) Access to encryption software is relatively easy, for instance by simply downloading it from the Internet.

2) It is difficult to prove beyond reasonable doubt that an accused has sent an encrypted message without prior authorization. Electronic communication on open networks is not like an end-to-end telephone conversation, where people can be identified by, for instance, their voice, and

3) Encryption is also possible using steganographic methods. These methods allow one to hide a messagein other data (e.g. images) in such a way that even the existence of a secret message and thus the use of encryption cannot necessarily be detected.

As a result, restricting the use of encryption could well prevent law-abiding companies and citizens from protecting themselves against criminal attacks. It would not however totally prevent criminals from using encryption. Most of the few criminal encryption cases that are known and used for justifying governmental regulation of encryption concern “professional” criminals or terrorists. However, it is unlikely that such parties would be stopped from using this technology even if regulations would prohibit them from doing so (cf. Denning & Baugh, 1997).

Some agencies have suggested the use of TTPE (see Table 1 for a definition of the term) to reduce misuse of encryption. The purpose of TTPE systems is to preserve the ability of the intelligence and law enforcement agencies to access and decrypt information if necessary to fight crime and terrorism. With the help of TTP, procedures for disclosure to such agencies of encryption keys are established. However, such an approach faces two major challenges:

(1) the sheer volume of keys to be stored over time assuming a wide use of encryption technology by consumers, medical and other organizations as well as governments;

(2) trans-national concerns whereby a person or organization's communication is decrypted in another country by a law enforcement agency that would not have been given these keys under a more democratic regime (e.g., unless court order was provided).

Public key infrastructures will probably result in a nightmare for private and corporate users worldwide with substantial costs to be paid by users and misuse and abuse by unauthorized parties being an ever possible threat. Current discussions in France about legislative efforts for public encryption do not suggest a practical solution to this problem (e.g., http://www.freenix.fr/netizen/chiffre/advice-ce.html).

4. CONCLUSION

Comprehensive medical record keeping and the beginning of intelligent computer-based agents that can exploit patient records mark the beginning for, hopefully, further improving the quality and/or reducing the costs of health care for governments and people. Unfortunately, as this paper outlined for the reader, side effects such as privacy losses and misuse of information, as well as possible technical and social problems to data and information confidentiality, integrity and availability are numerous.

This paper discussed both technical and social issues as far as encryption and privacy of medical records are concerned. Specifically, how divergent stakeholder groups' interests might result in conflicts and how this could affect our possible success in limiting health care costs with the help of medical databases was outlined. Furthermore, how local and international regulation, or lack thereof, may further hamper the implementation of medical databases and their effective use in providing health care was discussed.

The issues discussed in this paper have implications for any large database used by organizations and governments around the world. Accordingly, while we focused primarily on medical databases, customer, supplier and investor/broker databases require the addressing of the same issues (e.g., technical, social and regulatory) as far as privacy of such data are concerned. Below we discuss practical implications in some more detail.

4.1. Implications for Security Professionals

This paper indicates that security professionals are faced with many challenges as far as privacy, encryption and security of databases are concerned. The increasing use of public networks offers the possibility for more and new business, creating new channels of distribution and new methods of reaching the customer. However, the noticed threats and vulnerabilities to information management using technology currently threaten the realization of such information opportunities. Additionally, confidentiality, integrity and availability of databases must be questioned, while privacy for citizens and consumers is threatened. As outlined in this paper, these factors pose a risk to information for security professionals trying to implement and safeguard such information systems.

At this stage, the risks outlined here must be countered effectively; however, this seems to be the greatest challenge for all stakeholders (e.g., patients, doctors, regulators, information systems specialists and others). Insufficient or non-existing laws or regulations are currently the biggest impediment to the implementation of available state of the art technology. Such technology is withheld from the public-at-large by a small group of stakeholders (i.e., security and defense establishments), claiming that they do it to protect society.

Security professionals who are confronted with these problems should join initiatives that support the protection of privacy and the free availability of strong encryption technology. Security professionals should help these initiatives and citizens action committees in finding arguments, which, in turn, convince members of parliament to support legislation and regulation that are truly based on real users' requirements. Unfortunately, legislation and regulation is often based on proxy statements from intelligence or law enforcement forces, while legislators' understanding of these issues is stretched beyond comprehension and understanding of intended and unintended effects.

From the technology side of the coin, it is paramount that security professionals do understand that public key cryptography is not about confidentiality protection, it is primarily for digital signatures and the trusted distribution of keys. However, the principle of trust is only working as long as no third party is involved in the process. Neither does the involvement of a third party make sense from a business perspective since administration of many keys is a nightmare and would be extremely costly.

4.2. Implications for Public Policy Makers

The short review of regulatory developments as presented here does not provide the reader with a comprehensive review of the many issues involved. Nevertheless, the overview indicates that regulatory efforts are still lagging behind the technical developments of e-commerce and use of the Internet for communication purposes. Worse is probably that international harmonization is non-existent for all practical purposes.

International treaties, constitutions and laws guarantee the fundamental right to privacy (e.g., Privacy International, 1996). Treaties, constitutions and laws guarantee the communicating parties the right to secrecy of such communications (e.g., European Commission, Telecommunications, Information Market and Exploitation of Research, October 1997; No Author, October 8, 1997). The debate on the free availability of strong encryption technology (or the limitation of it) directly affects the individual right for the protection of privacy and the requirements for data protection for electronic commerce.

Strong encryption technology without key escrow or key recovery offers fundamental protection to those who seek to bring official abuses of power to light. Any restrictions on use of encryption would create opportunities for the violation of free expression for individuals in countries where dissent is punished. Dissidents and human rights organizations under repressive regimes use encryption technologies to share their concerns and transmit information which is often sensitive. Encryption has the power to authenticate the identity of these authors to their partners abroad, and protect their identity from despots at home. Any key escrow mechanism will result in loss of confidence among groups and individuals, mostly based in repressive regimes. This would mean a tremendous blow to international efforts to support the cause of human rights (Akdeniz, 1998).

4.3. Implications for End-Users and Consumers

For end-users and consumers or patients, the picture is not very rosy either. It will be difficult to convince legislators, politicians and organizational interests (e.g., insurers and health care managers) to abandon their ideas for national information systems about citizens and their respective health data files. The realization of such a huge database may ultimately violate people's privacy or at least invade it necessarily (to save their life) or unnecessarily (e.g., data about venereal diseases ends up in the local newspaper). Worst of all, if non-authorized parties obtain such data, criminal activities may be the result (e.g., extortion from some citizens by some groups based on information obtained from their medical records).

Regulators have been concerned about illegal use of encryption technology by a very small group of people who will use the best technology regardless of what regulators might have put on the books. Nevertheless, politicians striving for containing health care costs by using information technology may have been too pre-occupied with technology matters, thereby forgetting that the most obvious approach of charging user fees may result in much bigger gains. Accordingly, user fees will reduce unnecessary doctor visits, while different health care charges for non-smokers and people who exercise regularly may result in huge economic savings well beyond the few million dollars saved with information technology. Naturally, user fees should not apply to certain groups to assure doctor visits where needed (e.g., for children and people on welfare). More importantly, such a policy will likely improve the quality of life for many while restricting medical information to the caregivers that need such information. In turn, people's privacy will be far better protected than it will ever be if we implement national health care databases.

For citizens and consumers, the challenge will be to make their concerns heard by legislators and interest groups (e.g., industry) alike. Unless action committees and voters start lobbying their parliament representatives now and put privacy, encryption and health information disclosure issues at the top of legislative agendas, they will ultimately be faced with an environment not reflecting their wishes, needs and desires. Leaving such issues to politicians and various stakeholder groups, including lobbyists, will come to haunt consumers and citizens in the future. Accordingly, this may be the last opportunity to change the direction of a running train not following democratic principles nor adhering to the wishes of majority.

4.4. Conclusion

While information professionals and researchers wrote this paper, our conclusions would indicate that we are not necessarily willing to run down a dead-end alley. While we believe in the advantages of information technology, we are afraid that its unwise application with national health information systems without considering regulatory implications (nationally and internationally) while leaving human behavior and interests out of the equation, is politely put, dangerous if not outright negligent and irresponsible.

We urge all parties to carefully balance economic, political, and individual concerns, as well as ethical and moral issues about safety, security, privacy and economic concerns when discussing the feasibility of large-scale medical databases. The concerns outlined here might overshadow any small economic benefits that might be gained through such information systems. Thus it is each reader's responsibility to protect and secure privacy and confidentiality issues by advancing these issues and insisting on the right of each citizen to encrypt his or her communication without third party interference.

REFERENCES

Abelson, H., Anderson, R., Bellovin, S.M. Beneloh, J., Blaze, M., Diffie, W. Gilmore, J., Neumann, P.G., Rivest, R.L., Schiller, J.I., Schneider, B. (1997). **The risks of key recovery, key escrow, and trusted third-party encryption**. (ftp://research.att.com/dist/mab/key_study.txt) (July 1, 1997).

Akdeniz, Y. (1998). **No chance for key recovery: Encryption and international principles of human and political rights**. Working Paper, University of Leeds, UK.

Anderson, R. (January 12, 1996). **Security in clinical information systems**. (http://www.cl.cam.ac.uk/ftp/users/rja14/policy.txt) (January 23, 1998).

Avrahami, R. (October 6, 1996). List sale case to the VA Supreme Court. **Computer Privacy Digest, 9**(23), pp. 3-4 (<comp-privacy@uwm.edu>)

Bill 68 1993, Chap. 17 (August 4, 1993). An act respecting the protection of personal information in the private sector. **Gazette Officielle du Québec**, 125, 4253-4279.

Blaze, M., Diffie, W., Rivest, R.L., Schneier, B., Shimomura, T., Thompson, E., Wiener, M. (1996). **Minimal key lengths for symmetric ciphers to provide adequate commercial security.** (ftp://research.att.com/dist/mab/keylength.txt) (July 10, 1997).

Bloom, P.N., Milne, G.R. & Adler, R. (1994). Avoiding misuse of new information technologies: Legal and societal considerations, **Journal of Marketing,** 58, 98-110.

Bundesministerium fuer Bildung, Wissenschaft, Forschung und Technologie (October 8, 1997). **Verordnung zur digitalen Signatur** (Signaturverordnung – SibV). (Regulation for digital signatures) (http://www.iid.de/rahmensigv.html) (February 28, 1998) (unofficial English translation can be found at http://ourworldcompuserve.com/homepages/ckuner).]

Council of Ministers (August 5, 1997). **Schema di Regolamento Atti, documenti e contratti in forma elettronica** (regulatory framework for electronic documents and contracts in electronic form). Approved by the Italian Council of Ministers.

Council Regulation (EC) 3381/94, (December 19, 1994) **Setting up a community regime for the control of exports of dual-use goods**, OJ L 367/1, 31.12.94. Council Decision 94/942/CFSP, 19.12.94 establishes the lists of dual-use goods covered by the Regulation, OJ L 367/8, 31.12.94.

Coughing up. (1997, October 25). **The Economist**, p. 94.

Cryptographic **algorithms** (not dated). (http://www.cs.hut.fi/ssh/crypto/algorithms.html) (Accessed July 15, 1997).

Culnan, M. J. (1993). “How did they get my name?”: An exploratory investigation of consumer attitudes toward secondary information use. **MIS Quarterly,** 17, 341-363.

Directive of the European Parliament and the Council (adopted by the Council on 24th of July, 1995). On the protection of individuals with regard to the processing of personal data and on the free movement of such data (final). Bruxelles: The Author.

Denning, D. E., & Baugh, W. E. Jr. (1997). **Title of article** (http://guru.cosc.georgetown.edu/~denning/crypto/oc-abs.html) (December 15, 1997)

Donaldson, T. & Preston, L. (1995) The Stakeholder Theory opf the Corporation: Concepts, Evidence and Implications. **Academy of Management Review,** 20(1), pp. 65-91.

Doss, E. & Loui, M.C. (1995). Ethics and the privacy of electronic mail. **The Information Society, 11**, 223-235.

DTI (1997). Licensing of TTPs for the provision of encryption services **- DTI Public Consultation Paper** # *3.* Brussels: The Author (http://www.dti.gov.uk/pubs/) (December 17, 1997).

European Commission, **Telecommunications, Information Market and Exploitation of Research** (October 1997). Ensuring security and trust in electronic communication. Brussels: The Author (COM(97)503

Freeman, R. E. (1984) **Strategic Management: A Stakeholder Approach**. Boston, MA: Pitman.

Gattiker, U. E. & members of EICAR Working Group 1. (1997). Internet security: Strategic and social issues. **Proceedings of the European Institute for Computer Anti-Virus Research (EICAR) 1997 Security Workshop, Hamburg, Germany** (pp. 173-211) (see also http://www.eicar.com/wg1.htm).

Gattiker, U. E., & Kelley, L. (1998). Morality and computers: Attitudes and differences in moral judgments across populations. **Information Systems Research** (currently being revised).

Gattiker, U. E., Kelb, J., Janz, L., Holsten, H., Greshake, J., Schwenteck, O., & Miller, J.(1997). Direct marketing and privacy for telephone and internet users: A South African field study. **Global Business in Practice. Proceedings of the Tenth International Bled Electronic Commerce Conference, Bled, Slovenia,** 604-639.

Giussani, B. (1998, 24. February). An Appraisal or technologies of political control. **Eurobites**, p. 1.

Gostin, L. O., Lazzarini, Z., Flaherty, K. M. (not dated) **Legislative survey of state confidentiality laws, with specific emphasis on HIV and immunization**. (http://epic.org/privacy/medial/cdc_survey.htm) (July 18, 1997).

Information Policy Committee, National Information Infrastructure Task Force (April, 1997). **Options for promoting privacy on the national information infrastructure**. (http://www.iitf.nist.gov/ipc/ipc-pub.html) (July 22, 1997).

Katsh, E. (1994). Privacy and new information technologies. Paper delivered to 18th **Regional Conference the History and Philosophy of Science**, University of Colorado, Boulder, Co.

Loi N° 90-1170 (29 December 1997). Article N° 28. Telecommunications law. (http://www.legifrance.fr) (Accessed March 1, 1998). This law is currently being modified according to loi N° 96-659, 26.7.96 de réglementation des télécommunications art 17; (http://www.telecom.gouv.fr/ francais/activ/telecom /nloi17.htm) (December 17, 1997)

Harwood, R.L. (1990). Perceptions of social responsibilities in India and in the United States: Moral imperatives or personal decisions?, **Journal of Personality and Social Psychology,** 58, 1, 33-47.

McClosky, H. & Brill, A. (1983). **Dimensions of tolerance: What Americans believe about civil liberties.** New York: Russel Sage Foundation.

Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a theory of stakeholder identification and salience: Defining the principle of who and what really counts. **Academy of Management Review**, 22, 853-886.

Wassenaar arrangement on export controls for conventional arms and dual-use goods and technologies (December 20, 1995). (**(http://ideath.parrhesia.com/wassenaar/wassenaar.html**) (March 4, 1998)

Striking the right balance. Access to health informtion (December 5, 1996) (http://www.health.gov.ab/access.htm) (July 21, 1997).

Government introduces draft legislation to protect the privacy of health information. (June 11, 1997). (http://www.gov.ab.ca/~pab/4984.html) (October 28, 1997).

Strategic partner selected to develop a blueprint for an Alberta health information system. (July 14, 1997). (http://www.gov.ab.ca/~pab/5130.html) (October, 28, 1997).

Sequoia Software chosen to link U.S. patient records. (October 24, 1997). (http://www.microsoft.com/industry/health/press/Sequoiapr.htm) (January 23, 1997).

Towards a European framework for digital signatures and encryption. **European Internet Forum Policy Papers** (October 8, 1997) (http://www.ispo.cec.be/eif/policy) (October 13, 1997).

The people vs. AOL. **Adbusters. Journal of the Mental Environment**, (Winter 1998). No. 20, p. 60.

OECD (1997). **Report on background and issues of cryptography policy**. Paris: The Author.

OECD (November 1980). **OECD Guidelines governing the protection of privacy and transborder flows of personal data**. Paris: Author.

Pitchford, R. A., & Kay, S. (1995). GP practice computer security survey. **Journal of Informatics and Primary Care**, September, 6-12.

Privacy International. (1996). The Universal Declaration of Human Rights. URL:http://www.privacy.org/pi/intl_orgs/un/intl-decl-human-rights.txt (February 11, 1998).

Schlossberg (1993). Victims tired of researchers getting away with murder. **Marketing News**, August 16, A16, 1.

Spriggs, M. T., & Nevin, J. R. (1996). Negative option selling plans: Current forms versus existing regulations. **Journal of Public Policy & Marketing**, 15, 227-237.

Swiss police have secretly tracked the whereabouts of mobile phone users via a telephone company computer… (as reported in a Swiss Sunday newspaper). No Author (Dec 28, 1997) **Reuters**.

Szlovits, P., Doyle, J., Long, W. J., Kohane, I., & Pauker, S. G. (May 1994). **Guardian angel: Patient-centered health information systems.** (http://medg.lcs.mit.edu/project/ga/publications.html) (July 19, 1997).

Thorel, J. (18 December, 1997). Frenchy Cryptosoap #123578. **Lambda**, 3.08, p. 1 (see also http://www.freenix.fr/netizen/chiffre/avis-cssp.html).

Ulhøi, J. P. (1997) A stakeholder approach to green innovation. **In Proceedings of The Fourth International Meeting of the Decision Science Institute**, Sydney.

Ulhøi, J. P. & Madsen, H. (1998) Greening of industry in a push-pull stakeholder perspective. Theory, experiences and implications **Journal of Organizations & the Environment**.

van Swaay, M. (1995). The Value and Protection of Privacy. **Computer Networks and ISDN Systems, 26** (Suppl. 4), 149-155.

Walsh, G. (October 1996). **The Walsh report**. (http://www.efa.org.au/Issues/Crypto/Walsh/Walsh.htm) (August 31, 1997).

Wright, S. (1997??). **An appraisal or technologies of political control. Bruxelles**: European Parliament, Scientific and Technology Options Assessment (STOA)