IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Hershey PA 17033-1117, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4199

New Challenges in Privacy Protection

Lech J. Janczewski
The University of Auckland, New Zealand, Department of Management Science and Information Systems, Auckland, New Zealand
Tel: 64 9 373 7599, Fax: 64 9 373 7430, lech@auckland.ac.nz

ABSTRACT

The protection of privacy is a function of many variables: culture, politics, and point of view. Practically all countries have introduced laws regulating these problems. Terrorist attacks cumulating with the destruction of the World Trade Centre in New York and the Pentagon in Washington indicated a need to change these regulations. This paper therefore defines the notion of privacy, cites typical regulations related to the protection of privacy and the interception of private communications and documents. This discussion terminates with a presentation of a worldwide prognosis on this field.

INTRODUCTION

The attack against major US businesses and military facilities on September 11th, 2001 had and has a major effect on the way the entire civilised world functions. During the writing of this paper it is impossible to predict the final outcome of military actions launched against the people responsible of the attack or those who sheltered them. However, without a doubt, we expect a major shift in the attitude towards protection of the interests of individuals. Therefore, this paper will examine the present state of privacy protection in certain countries of the world and a prognosis will be presented about the direction of possible changes in this field.

In the past the focus of the law was aimed on protecting the privacy of individuals through setting up standards related to spreading the contents of paper documents relating to individuals and the interception of traditional mail. Growing utilisation of the Internet, and more generally, computer systems and networks made most of these regulations non-functioning.

The best illustration of this is in the information related to the operation of Osama bin Laden's al-Qaeda network. French police in Paris intercepted a scribbled notebook belonging to a suspected master bomber. FBI and French computer experts studied the Arabic script and are convinced that terrorist cells have been using codes to disguise their electronic mail and to hide maps and instruction on sports chat rooms, pornographic websites and photographs sent over the Internet. Hence, intelligence agencies are certain that al-Qaeda uses electronic camouflage to keep in touch with its network of agents (Zalewski, 2001).

On one hand we have witnessed the growing utilization of computer networks for conducting fraud operations and on the other; the growing concern of society becoming aware that their privacy could be the first victim of the "War with Terror". All the indicators show so far computer fraud and illegal access to information are on the rise. This trend is clearly seen in the "CSI/FBI Annual Security Report" prepared jointly by the Computer Security Institute and the Federal Bureau of Investigation (CSI/FBI, 2001). According to this report, for the last five years the losses resulting from computer/network abuse, are on an increase.

The position of the author of this paper is not to judge what level of protection for individuals should be minimal or maximal (at present), nor whether it is moral or not to read somebody's private correspondence. The object of this paper was rather to present:

- The mechanisms that currently exist around the world in this field,
- The public perception of these mechanisms,
- The demonstrated tendencies,
- What they could mean for the world community.

DEFINITION OF PRIVACY

Almost every author on this subject introduces his or her own definition of privacy or rather "information privacy". For instance, Gunasekara, (2000), defines it as 'an ability to control information about oneself". Obviously, the right to privacy needs must be balanced against competing social and individual rights. This is illustrated in Fig 1, where privacy is a point on a line between individual and society needs. There is no general answer about where this point should be located; this depends on the customs, political regime, or the nature of the information. It is obvious that more autocratic governments try to push the privacy point closer to the society (i.e. to give more protection to society at the individual's costs), contrary to the more democratic-type government. The position of this point is also a function of who is in charge of setting it up: the individual, a society at large or a group of individuals (like law and order agencies).

COMPONENTS OF THE PRIVACY CONTROL

The law regulating privacy control varies from country to country, but some similarities exist in most of the developed countries. These foundations of privacy are as follows:

Privacy Law

These are acts of the local parliaments regulating the distribution of information related to individuals. Usually individuals have rights to verify information about them and to set up limitations related to the spreading this information. Typically, privacy acts allow information disclosure in the case of "important social reasons".

Illegal Access to Computer Records

This law is usually labelled as "Anti-hacking Law". These acts introduce penalties for individuals attempting unauthorised access to computer-stored information. Typically the law differentiates the penalties on the basis of the level of damage caused by an illegal activity. This could range from unauthorized attempts to access a resource through to more serious such as changes to, or destruction of records.

Telecommunication Law

These are the rules of running telecommunication networks. Among these laws are clauses related to the rights of organisations managing networks to monitor/control the content of transmitted messages. Typically the telecom organisation has rights only to collect information related to the payment for such services.

Crime Acts

In some countries there is no separate law for regulating access to computer networks and parts of the "anti-hacking law" are incorporated into this type of legislation.

Investigation Agencies Law

The majority of countries have introduced laws regulating the operational principles of agencies like FBI, Scotland Yard, Securité, etc. Obviously, the law varies from country to country, but the final conclusions are the same; in the case of suspicions that an individual

This paper appears in *Issues and Trends of Information Technology Management in Contemporary Organizations,* the proceedings of the Information Resources Management Association International Conference.

may be engaged in criminal activity, tapping of that person's contacts (either electronic or traditional) can be authorised. The law usually states which agency is authorised to do the tap, technical conditions of doing so, and who would decide about launching such activities. The last point is especially sensitive and usually authorities outside of the investigating agency grant the decision.

It is worth noting that to enhance the across-border co-operation of law enforcement agencies a considerable effort is currently being undertaken to standardize the above regulation on a world scale. The countries currently participating in this are the European Union, USA, Canada, Norway, Australia and New Zealand.

REVIEW OF PRIVACY LEGISLATION

A country with well-developed privacy legislation is New Zealand. The principle act governing privacy there is the Privacy Act (1993) introduced in 1993. The essence of the Act is 12 Privacy Principles listed below:

1. Personal information is only to be collected for a lawful purpose, which should be connected with a function or activity of the agency.
2. Information should be collected directly from the individual concerned.
3. The individual concerned should be aware that information is being collected and should know:
   - The purpose for which the information is being collected;
   - Who are the intended recipients of the information;
   - The consequences for the individual if the information is not provided;
   - The rights of access to and correction of personal information provided.
4. Personal information shall not be collected by unlawful, or unfair, or intrusive means.
5. Information is protected by security safeguards against loss, unauthorised access, use, disclosure or modification.
6. The individual concerned shall be entitled to obtain confirmation that information is held and access to information is held.
7. The individual concerned shall be entitled to request correction, or a statement that such a change request has been made, to information held.
8. The holder of personal information must check its accuracy before use.
9. The holder of personal information may not keep the information for longer than necessary.
10. Information may only be used for the purpose for which it was originally intended.
11. The Holder of personal information may not disclose the information to any other person or agency.
12. The Holder of personal information may not assign a unique identity (key) unless it is necessary to carry out its function, nor may that identifier be that already used by another Holder.

The most important point from the above list is No 5. The meaning of the point is that an agency storing personal information must take appropriate measures to protect the data against unauthorised changes and disclosures. Of course, in the text of the act there are numerous notes explaining that in specific situation the custodian of the information could release this information.

The authors of the New Zealand Privacy Act were aware of society's demands to handle properly the "Big Brother Symptom", in other words, making record matching difficult. This is seen through the introduction of the 12p of the Privacy Principles. The meaning of the point is that a key developed for specific task cannot be used for other database, like Inland Revenue Department Identifier (or equivalent) cannot be used for issuing driving licences.

REVIEW OF THE ANTI-HACKING LAW

Privacy law is usually very general and most countries have introduced similar acts regulating the protection of privacy in specific sectors of their society. For instance in New Zealand, (the mentioned before) Privacy Act was closely followed by a similar regulation related to the medical sector (Medical Act, 1994).

Regulations governing penalties related to the unauthorised access to computer records, however, are set up differently across the world. There are countries where such an act is a crime, like in the USA, under so called "1986 Computer Fraud and Abuse Act", (Graham, 2000), contrasting with, for instance, New Zealand, where there is no direct parliamentary act punishing hacking or similar activities. The IT community of New Zealand for a long time has been warning the government about the consequences relating to such an omission and finally during November 2000 a "Crime Amendment Bill No 6 with Supplementary Order Paper No 85" was finally tabled in the NZ parliament (SOP no 85, 2000). Despite the urgency of fixing this legislation hole, up to the time of writing this paper (January 2002), the act was not voted by the Parliament.

A review of the way of assessing unauthorised access to computer records was done and shows that there are significant differences in the definition of such activities. Under some laws, only unauthorised changes could be the subject of prosecution, while unauthorised access without introducing any changes could not be punishable. These differences make co-ordination of efforts in tracing most of these international hackers difficult. The best way to illustrate this would be the case of the Philippine student who developed and spread the famous Love Bug virus. As it was reported on TV (Prime, 2000), the Philippines authorities arrested the culprit but released him quickly, as there was no law there to imprison him.

REVIEW OF THE INVESTIGATION AGENCY LAW

As a result of the September 11th, 2001 attacks legislation related to the powers of agencies investigating crimes is undergoing the most rapid changes. (Please note that in this review we are not discussing such cases as in the PR of China or the Russia, where all the Internet traffic, by definition is read by the investigating agencies). The summary of the situation up to January 2002 looks as follows:

Perhaps the most stringent law has been introduced in United Kingdom through the "Regulation of Investigatory Powers Act" of 2000 called the RIP Act. (RIP, 2000). The Act regulates (among many issues) the procedure of obtaining by the police the rights to intercept and read private messages (both in the traditional and in the electronic form). The first part of the document introduced the concept of the unauthorised and authorised interception and states that interception of private mail without a warrant is a serious crime. A warrant signed by the Secretary of the State or in an urgent case by a senior official (explicitly authorised by the Secretary) is necessary to launch the interception procedures. Each warrant is limited to a specific case and person. Under the RIP Act the authorities may demand the release of the encryption key of the messages being subject of the interception. The RIP Act also regulates the financial issues related to the execution of the interception warrants, especially between the local ISPs and MI5 (UK Government Agency designated to managed the interception procedures).

In USA a different approached has been adopted. The foundation of the interception activities is a diagnostic tool developed by FBI to intercept private electronic communication, popularly called the "Carnivore Box". Basically it is a sniffer tool, which can read addresses or addresses and contents of Internet messages. The tool is in the form of hardware and associated software unit owned and run by FBI, installed at an ISP site. There are detailed procedures of obtaining permit to use the box. The FBI claims that the tool was used around 25 times leading to up to August 2000 (Graham, 2000).

As a result of the September 11th, 2001 attacks many countries have revised their security policies, which in turn will affect the rights of individuals, related to the privacy of their telecommunications. For instance, Germany introduced two sets of proposals, on December 8th 2001 and on December 14th, 2001. The first set includes (among other things) plans to increase spending by $1.4 billion on security and to

crack down on some extremist religious groups. Under the second, the German's Office of the Protection of the Constitutions and the Federal Intelligence Service would be able to request information on suspects from banks, airlines and other organisations. On both the national and state level, the Office would be able to request information about political opponents from outside the country (Frankfurter Allgemeine, 2001). These new powers, without a doubt, would decrease protections of individual communications from government tapping. Similar legislation has been introduced in many other countries.

In some sense, the reaction of the public for these new security measures is fairly restrained. Apart from a few demonstrations organised by civil libertarians, the public has accepted the new polices. The author of this paper still remembers the fierce discussion rolling through the USA in the 50s against use of safety belts in cars. The main argument was that compulsory belting up violates the rights of individuals. This time however, the public ready to accept the necessity of introducing these measures. For instance popular magazines inform the public how to deal with these new policies (USA Today, 2001).

THE PROGNOSIS

Events starting with the September 11th, 2001 attacks showed the world the vulnerability of the Western society to the activities of a limited number but financially independent terrorists groups. These groups enjoyed relatively wide freedom of action despite not hiding their objectives. The initial successes of these groups were based on the practically nonexistent security measures related to public life like: transport, telecommunication, and businesses activities. In this situation the choice was clear: maintain high level of personal freedom of individuals with high risk of terrorist attacks or, in the interest of the safety of the society, introduce some significant limitation to it. Generally, the second alternative seems to be adopted.

The number of actions launched varies from introducing more widespread and more detailed security checks at airports, through to close watch of all extremist groups, to freezing accounts of people or organisations suspected of supporting the terrorist movements.

Privacy protection is usually governed by the law and the introduction of changes to the existing parliamentary acts takes time and one may expect that changes to the privacy legislation should emerge within a year or two.

On the other hand, mass implementation of information technology in processing documents requires introduction of laws legalizing documents stored in soft form. Parallel to that is the introduction of technologies, procedures and organization able to police this law. This practically means introduction of legal definition of digital signatures, validity of electronic documents and contracts and setting up an adequate "Advance technology police" able to handle the computer-assisted crime. Privacy protection regulation without being supported by these regulations would no make sense.

All the above factors allow the formulation of the following long terms prognosis:

- More and more countries will soon introduce law defining the validity of documents generated and stored in electronic form, especially regarding the format of digital signatures. This should lead to the situation were soft documents would attain the same level of recognition as hard copy documents.
- There will be intensified international efforts to harmonize the countries' law related to electronic documents. A number of issues need to be resolved very quickly; like the country of origin or date of signing a contract. For instance Europe is separated from New Zealand by a 12 hours gap. Contract signed between parties residing in New Zealand and France would have two different dates. Besides, where was the contract signed?
- Government agencies will receive more power in launching investigations including the interception of electronic mail and documents stored in electronic form. The most probable course of action is the adoption of solutions similar to that already existing in the RIP Act, discussed earlier in this paper. When the RIP Act was introduced it was met with strong criticism from many. In view of the present situation, the opposition would be much milder.
- Restriction regarding the export/import of strong cryptography has not worked in the past and one may expect further removal of these limitations. However, the investigating authorities must have access to the encrypted records and in the opinion of the author the introduction of a law stipulating the release of the cryptographic key in specific situations is inevitable.
- All known Privacy Acts contain clauses stating that specific data about individuals could be released if it is in the benefit of society. After the September 11th, 2001 this means that these clauses will be applied more often and more liberally…

REFERENCES

Zalewski, T., 2001, *Front wewnetrzny (Internal front)*, Polityka, No 41, 2001

CSI/FBI Report, 2001, *Computer Crime and Security Survey*, http://www.gocsi.com/prelea/000321.html

Gunasacrra, G., 2000, *Protecting Personal Privacy in Cyberspace: The Limitations of Third Generation Data Protection Laws Such as the New Zealand Privacy Act 1993*, in Internet & Intranet Security Management: Risks and Solutions, IDEA Group Publishing, 2000

Privacy Act, 1993, *Privacy Act*, http://www.knowledge-basket.co.nz/privacy/slegisf.html

Medical Act, 1994, *Health Information Privacy Code 1994*, http://www.knowledge-basket.co.nz/privacy/comply/HIPCWWW.pdf

R. Graham, *Carnivore FAQ*, http://www.robertgraham.com.pubs/carnivore-faq.html

SOP no 6, 2000, Crimes *Amendment Bill No 6, SOP Number 85*, House of Representatives, New Zealand Parliament, 7 November 2000

Prime, 2000, *Cyber Attack*, Prime TV, Auckland, New Zealand, 20.07.2000

RIP, 2000, *Regulation of Investigatory Powers Act*, http://www.legislation.hmso.gov.uk/acts/en/2000en23.htm

Carnivore, 2001, *Carnivore Diagnostic Tool,* http://www.fbi.gov/hq/lab/carnivore/carnivore.htm

Frankfurter Allgemeine, 2001, *Parliament Backs New Security Bill*, editorial, No 292, 2001

USA Today, *Frisking becomes invasive*, editorial, December 14-16, 2001