24th International Data Protection and Privacy Commissioners Conference

Cardiff 9th – 11th September 2002.

Issues Arising from September 11th 2001

Canada (Ontario)

Canada (Quebec)

Czech republic

Denmark

France

Greece

Guernsey

Hong Kong

Hungary

Iceland

Ireland

Isle of Man

Jersey

The Netherlands

New Zealand

Norway

Spain

Sweden

Switzerland

Thailand

United Kingdom

Canada's Response to the events of September 11, 2001

Ann Cavoukian, Ph.D., Information and Privacy Commissioner/Ontario

The events in the United States on September 11, 2001 caused the federal government to examine all measures available to protect the safety and security of Canadians. As an initial response to these events, the Government of Canada introduced the Anti-terrorism Act, which amended the Criminal Code, the Official Secrets Act, the Canada Evidence Act, the Proceeds of Crime (Money Laundering) Act and other statutes. The legislation amended the Criminal Code to implement international conventions related to terrorism, to create offences related to terrorism, including the financing of terrorism and the participation, facilitation and carrying out of terrorist activities, and to provide a means by which property belonging to terrorist groups, or property linked to terrorist activities, can be seized, restrained and forfeited.

It also amended the Official Secrets Act, which became the Security of Information Act. It addressed national security concerns, including threats of espionage by foreign powers and terrorist groups, economic espionage and coercive activities against émigré communities in Canada. It amended the Canada Evidence Act to address the judicial balancing of interests when the disclosure of information in legal proceedings would encroach on a specified public interest or be injurious to international relations or national defence or security.

The legislation amended the Proceeds of Crime (Money Laundering) Act, which became the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. Additionally, the legislation amended the Access to Information Act, Canadian Human Rights Act, Canadian Security Intelligence Service Act, Corrections and Conditional Release Act, Federal Court Act, Firearms Act, National Defence Act, Personal Information Protection and Electronic Documents Act, Privacy Act, Seized Property Management Act and United Nations Act.

The federal government also introduced Bill C-42, the Public Safety Act. Negative reaction to the Bill's wide scope was such that the Bill was withdrawn, replaced by Bill C-55 the Public Safety Act. Bill C-55, which has received first reading, amends 20 existing Acts, and will implement the 1975 Biological and Toxin Weapons Convention.

Further, in response to American requirements, the government introduced and quickly passed Bill C-44 An Act to amend the Aeronautics Act. The legislation permits Canadian airlines to disclose information about their passengers to foreign governments. The federal government pledged $7.7 billion over the next five years to improve security (mostly directed at strengthening border crossings and ports, together with immigration and transportation safety initiatives). The Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) will play a significant role in these initiatives. For more information, see the Safety and Security for Canadians Web site: www.gov.on.ca/MBS/english/new/protecting.html

The Province of Ontario also had several responses including the appointment of two new security advisors – former RCMP Commissioner Norman Inkster and retired Major-General Lewis MacKenzie – to strengthen Ontario's security. The Minister of Public Safety and Security also announced the appointment of a new Commissioner of Public Security.

Ontario also passed legislation to increase the security of vital documents such as birth certificates. Further, the government announced $9.5 million for four anti-

terrorism initiatives, part of a broader approach to counterterrorism involving security measures and a comprehensive review of emergency preparedness. For more information, see the Protecting Ontario Web site: www.gov.on.ca/MBS/english/new/protecting.html.

Canada (Ontario)

REPORT ON THE IMPACT OF SEPTEMBER 11TH ON DATA PROTECTION AND PRIVACY LEGISLATION IN THE PROVINCE OF ONTARIO, CANADA

Federal Security Legislation

In Canada, jurisdiction over criminal law and national security is a federal responsibility. As a result, the majority of legislative activity responding to September 11th in Canada has been at the federal level. This was primarily in the form of two pieces of legislation, the Anti-Terrorism Act (Bill C-36) and the Public Safety Act (Bill C-55). The lead in responding to the privacy issues raised by these bills was taken by my federal colleague, George Radwanski. I did write to the responsible ministers to support Commissioner Radwanski's views and convey my concerns with the unwarranted expansion of powers authorized by the legislation.

Birth Registration Process

In Ontario, the provincial government passed amendments to the Vital Statistics Act to bring greater rigour to the birth registration process. Ontarians are now limited to only one birth certificate at a time and must provide the signature of a guarantor when applying for a certificate. Lost, stolen, destroyed or found birth certificates must be reported immediately and lost or stolen birth certificates will be immediately deactivated. Individuals who misuse birth certificates or supply false information on applications will face significant penalties.

In addition to addressing security concerns, these amendments have the potential to increase the privacy of Ontarians. Birth certificates are foundation documents, meaning that once in possession of a birth certificate, other pieces of identification can be acquired. By putting stricter controls on issuing certificates, and creating better inventory controls on certificate numbers, it will be harder for individuals to assume false identities.

STEPS

Following September 11th, I recognized that government respect for the principles of privacy suffered a major setback. Government officials acknowledge that privacy is important, but insist that, in light of the scale of the carnage on September 11, ensuring the public's safety and security has become paramount.

Historically, privacy and security have been treated as opposing forces in a zero-sum game. Such a view, by necessity invokes a balancing act, where the greater the gains for one side, the greater the losses for the other. This win/lose attitude poses a major threat for privacy, since the public's desire for safety and security is so high. Continuing the post 9/11 debate within this framework threatens the very foundation of privacy, leaving its future in question.

This is why, in June 2002, I issued a challenge called STEPS, standing for Security Technologies Enabling Privacy (www.ipc.on.ca/english/pubpres/papers/steps). Through the STEPS program, I called for a change in the security/privacy paradigm. There is no inherent reason why greater safety and security must come at the expense of privacy. By reframing the issue, we can take the necessary steps to improve both. If we start with a new premise – that privacy and security are two complementary sides of an indivisible whole, then we can design technologies that protect public safety without sacrificing privacy.

The STEPS challenge is aimed primarily at "solution providers" – the developers of technology and their industry associations. Privacy must be incorporated into the concept, design and implementation of their technology solutions. A recent example of a STEP in action is the airline passenger scanning technology developed by the U.S. Department of Energy. Through the use of 3-D holographic imaging, the scanner reveals objects hidden underneath passengers' clothing instead of displaying the entire body. The scanner is designed and deployed in a manner that addresses security requirements while minimizing the intrusion into personal privacy.

Canada (Quebec)

IMPACTS OF THE SEPTEMBER 11 EVENTS ON THE PROTECTION OF PERSONAL INFORMATION AND PRIVACY

New security measures regarding civil status

For many years, management and issuing of important documents such as birth, marriage and death certificates were under the responsibility of the ecclesiastical authorities of Québec parishes and cities. A few years ago, Québec presented a modern vision of citizenship and overhauled the system for issuing these documents. Thus, the Government of Québec has consolidated the entire administration of birth, marriage and death certificates under a single agency, the Director of Civil Status.

In the wake of the events of September 11, 2001, the Government of Québec conducted a thorough review of its civil status document issuing practices and applied new security measures, primarily intended to identify the applicants for these types of documents. The new system therefore obliges people who apply for a certificate to identify themselves by means of two documents issued by the Government.

A birth certificate recently issued by the Director of Civil Status is the only official document used to apply for a passport, claim pension allowances, obtain a driver's license, or register a child in elementary or secondary school, or even in CEGEP or university.

The threat of terrorism affects the security of society. For Québec, this obligation to conduct a painstaking identity check of applicants for civil status documents is an important step in the fight against terrorism and part of the government's plan to ensure public security.

Czech Republic

Impact of September 11 on the Czech Republic

The terrorist attacks of September 11, 2001 in the U.S. have influenced, like in many other states, the attitude towards the existing security measures and initiated discussions on the sufficiency of powers of the state security authorities as well as the need to moderate the personal data protection. Examples namely from Germany and Great Britain delivered inspiration that made politicians to start debate on strengthening competencies of the power authorities – the Ministry of Interior, the Ministry of Defense and the Security Information Service (BIS). The Office for Personal Data Protection reacted immediately through public appearance in the mass media and warned against imprudent weakening of the Personal Data Protection Act in favour of these power authorities. Nevertheless an amendment had been prepared to the respective act aiming at strengthening the powers of secret services, which finally was not adopted since no political unity of opinions on the necessity of this step was achieved. The original resolve of some politicians to give more powers to the security authorities and to bring down the level of the personal data protection was scaled down by some events when security risks were increased by infringements of the existing security measures (e.g. the case of an unauthorized person who infiltrated session of the National Security Council of the Czech Republic although the security service was present at the entrance, or another, when a woman journalist entered unnoticed the restricted airport area and even embarked an aircraft in Prague-Ruzyne, etc.). Similarly the need to protect the Radio Free Europe/Radio Liberty building located in the centre of Prague has drawn attention to that kind of security protection.

The Office for Personal Data Protection contacted some politicians whose opinions were moderate and warned against retreat from the protection of human rights and freedoms in favour of strengthening the powers and competencies of the intelligence services and power authorities. The Office often cited documents adopted by the Council of Europe expert committees – the Declaration of the Committee of Ministers on the fight against terrorism, and the Resolution No.1 of 24th Conference of European Ministers of Justice, as well as the Opinion 10/2001 of the Article 29 Data Protection Working Party established within the European Commission and opinion of CJ-PD experts, and provided politicians with such materials.

Nevertheless the syndrome of September 11 is used as a general argument in the cases where objective reasoning cannot be found - as it was the case of the last amendment to the Act on Banks. The banks have been given new competencies for collecting and processing of personal data including the so call sensitive data (special categories of data as defined in the Article 8 of the Directive 95/46/EC). By the lack of any factual reasoning some politicians and supporters of this amendment used this very argument: "the September 11 syndrome means that the need to collect sensitive data is inevitable for the fight against terrorism". The Office for Personal Data Protection has refused such argumentation asking the DG Internal Market of the European Commission for standpoint and preparing a proposal for a new amendment to the Act on Banks, which would fully respect the principles of the personal data protection laid down in the Directive.

Denmark

Note on the impact of September 11th in Denmark in the field of data protection

---

Following the events of September 11th the Minister of Justice introduced a draft bill concerning different initiatives in the fight against terrorism to Parliament.

The bill mainly focused on the following issues:

- Implementation of the UN International Convention for the Suppression of the Financing of Terrorism
- Implementation of the Security Council Resolution 1371 (2001)
- EU-initiatives in the fight against terrorism
- Other initiatives in the fight against terrorism (strengthening of the power of the police in the field of investigation, extradition and certain clarifications in the Penal Code)

Prior to the introduction the Ministry of Justice asked the opinion of the Danish Data Protection Agency.

The Agency in it's reply focused on two privacy points in the draft bill:

1. Telephone companies and Internet Service Providers (ISP) have to keep records of traffic data for one year (retention of traffic data, including information on e-mails)

2. Direct access for the police to telephone companies' information on listings (including information not available to the public)

The Agency had no comments regarding police access to telephone listings.

As regards to retention of traffic data the Agency stated that this would require special legislation (ad hoc legislation). The Agency also stated that the proposal raised fundamental privacy concerns. As the final decision on this proposal was a of a political nature the Agency made no further remarks in this connection.

Because of the special circumstances of the draft bill the Agency proposed to insert a revise-clause in the bill.

The act (with the revise-clause) was passed in Parliament in June 2002.

France

24th International Conference of Data Protection Commissioners

The situation post-September 11th in France

National Committee of Information Technologies and Civil Liberties (CNIL),France

1) The impact of the events of September 11th on the protection of personal data has been relatively moderate in France. This relative moderation can be explained by the fact that since 1986, France has had antiterrorist legislation, brought in as a result of a wave of terrorist attacks. This legislation allows for a centralisation of penal action when dealing with acts of terrorism, specialised tribunals to judge terrorist crimes and greater powers granted to the police in this sphere as compared to others. This legislation, which was passed by the Constitutional Council in its time, is no longer questioned. Similarly, since 1988, France has legislation concerning computer fraud applicable to computer virus cases, and since 1991, a specific legislation on surveillance which is applicable to internet activity.

2) After the events of September 11th, France brought in specific legislation on the conservation of the rights of data connection for police use. These measures were prepared, however, well before September 11th and were the subject of consultations with both the CNIL and the State Council. They were adopted in the form of a law relative to the «daily security» of October 31st 2001 and fix the length of rights of data connection to a maximum of one year, specifying that the navigation rights cannot be used for such purposes. To be implemented, they need to refer back to a decree from the State Council, taken after advice from the CNIL which must specify the length of access according to the abiding circumstances. In its official advice on this legal project the CNIL suggested that the rights of access should be fixed by the law itself, and not by a State decree, and should be limited to three months. This did not convince the government which quickly and almost unanimously passed these measures. The CNIL will, however, be examining the way in which they are implemented.

3) Finally, the government announced, in documents attached to a law concerning police procedure passed after the presidential and legislative elections in May and June 2002, its wish to facilitate direct access to a number of personal data files for the police, with particular mention of the files belonging to telecommunications operators and ISPs.

Vigilance is thus continuing to impose itself. In this period marked by the concern of strengthening public security in all its guises in France, the CNIL's mission - to express its opinion freely and publicly in order to inform the government and public opinion - seems particulary important.

Greece

There is no concrete legal reactions in Greece connected with the tragic events of September 11th. The reason is that the Greek Parliament had already passed a bill on 15th June, the Law No.2928 referring to the "Amendment of provisions of the Penal Code and the Code of Penal Procedure and other provisions on the protection of citizens from punishable actions of criminal organizations".

According to this bill "a sentence of imprisonment of up to ten years is imposed to any person who sets up or is included as member in a structured group with continuous activity, made up of three or more persons and seeks to commit felonies provided for by articles concerning, among others, forgery, violations concerning to explosive materials, sinking of ship, poisoning of springs and food, disturbance of safety of trains, ships and aircrafts and a lot of other criminal activities.

Most important on the data protection point of view is, that the bill expands a lifting of secrecy of correspondence and communications, during interrogative acts on criminal organizations, by maintaining the judicial guarantees already being in force.

Additional to that the bill anticipates the possibility of DNA Analysis for persons suspected for the above mentioned crimes. According to the bill, when there are serious indications that a person has committed a felony covered by this law, the judicial council may order DNA analysis with the purpose of establishing the identity of the perpetrator of such crime. The analysis is limited solely to the particulars that are absolutely necessary for establishing such identity and is carried out in a state or university laboratory. The defendant may request his own DNA analysis for his defense.

Guernsey

Aftermath of September 11.

The main effect of September 11th has been to heighten concern for compliance with anti-terrorism and anti-money-laundering legislation.

Compliance Officers at financial services organisations report being under pressure to tip the privacy balance in favour of the prevention and detection of crime (especially fraud and terrorism) against the protection of individual privacy.

There have been increased pressures to Know Your Customer and therefore to store more personal data that is needed purely for the identification of customers and the conduct of their financial affairs.

Concern has been expressed about subject access requests where the data subject may have had suspicious transaction reports filed against them and to disclose such reports might be regarded as a "tipping-off" offence.

In my guidance to data controllers, I have emphasised the benefits of transparency – i.e. telling all clients of the need for compliance with anti-money laundering legislation thereby mitigating any subsequent complaints of apparently unfair processing or unauthorised disclosures. I have worked closely with the Financial Services Commission to try to resolve any apparent conflicts between our respective regulatory regimes.

I should emphasise that to date I have not received any complaints from data subjects in that regard.

A Short Report on the

The Impact of the Events of 11 September Upon Data Protection and Privacy Legislation in the Hong Kong SAR

Presented by
Raymond Tang
Privacy Commissioner for Personal Data, Hong Kong SAR

at the
24th International Conference of Data Protection and Privacy Commissioners
Closed Session

9 September 2002, Cardiff, Wales

---

1 Introduction

The appalling nature and magnitude of the 9-11 events prompted the HKSAR Government to undertake a comprehensive review of security policies and measures. However, that review, and the subsequent action taken, has not had any major repercussions upon the privacy rights conferred upon individuals by the Personal Data (Privacy) Ordinance, at least not to this point in time.

2 The Hong Kong Context

I believe that privacy and security concerns are inextricably linked but that they are also contextual. In the Hong Kong context, the response of the government has been carefully measured to address local needs and local circumstance. Whilst recognising the need to re-inspect the efficacy of the security and intelligence framework, there has not been any reaction, which impact upon privacy rights and our established privacy regimen, which has remained largely intact one year after the events of 11 September. As well, the proposal by the Immigration Department to upgrade the Hong Kong Identity Card to a smart card has been subject to demands for rigorous safeguards that are a response to the privacy concerns of some legislators and the public at large.

The following factors, largely contextual, have given rise to a situation characterised by what might be termed a respectful coexistence between the security needs of the State and the personal data privacy rights of the individual. The balance that has been struck indicates that the public would take a dim view of any government policies that might have the effect of diluting their privacy rights.

- The SAR Government, through the Secretary for Security, does not regard Hong Kong as a high profile target for a terrorist attack.
- Research also indicates that residents and visitors alike see Hong Kong as a 'safe city', compared with cities of a similar size in other parts of the world.
- Hong Kong has a highly visible policing policy. Officers on foot patrol are the norm and not the exception.
- The citizens of Hong Kong are acclimatized to a society in which ID cards are an accepted part of everyday life. They have been in existence since 1947.

- Generally speaking, there is not the same level of apprehension among Hong Kong citizens towards terrorism. There are strong preventative measures but no security overkill. Terrorism in Hong Kong is seen to be time and place specific.
- Our experience and research leads us to the view that the citizens of Hong Kong are cognizant of their privacy rights, and hold them in esteem. Attempts from any quarter to diminish those rights would spark public outcry. Privacy is taken seriously in Hong Kong and Chinese and English language media reporting or commenting daily on privacy is commonplace.

3 Striking the Balance

Whilst privacy rights are vehemently guarded by the public, Hong Kong is committed to supporting the international fight against terrorism. The United Nations (Anti-Terrorism Measures) Ordinance in compliance with UN Security Council Resolution No.1373(2001) was passed on the 28th September 2001, although its passage was subjected to strong criticism from some legislators as being 'rushed through', conferring draconian powers on the government and opening the prospect of invasions of privacy.

The context of Hong Kong has weighed significantly in terms of striking a balance between the security interests of the State and the personal data privacy rights of the individual. The community's awareness of the ramifications of security overkill (thereby playing into the hands of terrorists by reducing the rights and freedoms of democratic societies) has enabled that balance to be practised. The formula is about right insofar as Hong Kong is concerned, although the approach may not be a universal paradigm.

Raymond Tang
Privacy Commissioner for Personal Data – Hong Kong SAR
9 September 2002 at Cardiff, Wales

Hungary

IMPACT OF SEPTEMBER 11TH IN HUNGARY

After the tragic events of September 11, Parliament enacted Act No. LXXXIII. of 2001. on the struggle against terrorism, the impending of money laundering and on some other restricting measures. (The statute was not only enacted because of September 11th but was also enacted because the Financial Action Task Force (FATF), in 2001 declared Hungary a non-cooperative country in the fight of money laundering - as a matter of fact, the decision of FATF was highly unreasonable.)

The Act authorizes the Government to take restricting measures against certain states, citizens, legal persons and other organizations of such states. These (mainly economic, commercial, financial) restrictions can be initiated by government decree; and must be based on a International obligation of the Hungarian Republic. The Act also increased the severity of the rules of former Acts concerning money laundering.

Act No. LXXXIII. of 2001. is based on the language of the second anti-money laundering directive - directive 2001/97/EEC. In accordance with this directive, Act No. LXXXIII. of 2001 extended the scope of financial institutions being under control. Right now, credit and financial institutions, auditors, external accountants and tax advisers, real estate agents, dealers in high-value goods, auctioneers, casinos are under the authority of the act. Notaries and legal professionals are also under the authority of the act but there will be a special statute enacted on the rights and obligations of people representing these two professions.

Costumer identification: According to Act No. LXXXIII. of 2001 the customer identification requirement is applied to each transaction involving cash in the amount of 2 million Forint, which is about 8 thousand Euro. The financial institution in Hungary is required to keep record of the customer identification for ten years, and also required to keep record of the customer who is a suspect of money laundering based on the judgement of the employee dealing with the customer. The financial institution identifies every customer who enters into business relation with the financial institution and keeps evidence of the identification for at least 10 years.

Data protection dilemma with the customer identification system: There will be data basis with thousands and thousands of personal data held for a non-identified future purpose: „criminal purpose", in specific for the prevention of money laundering. Such a preventive purpose for data could be unconstitutional according to the existing case-law of the Hungarian Constitutional Court.

Reporting system: According to Act. No LXXXIII. of 2001. every suspect of money-laundering shall be reported to the Police. The Police examine each reported case.

Iceland

I. Short response on the impact of September 11th.

Iceland is fortunate in having a political system based on respect for fundamental human rights and principles such as personal privacy. The events of September 11th have however put these rights and freedoms in a new perspective and reminded us of the importance of being on guard against attempts to undermine them.

To begin with let me report in the reactions of the Icelandic authorities:

a) The government commanded that greater security measures should be implemented at Keflavik International Airport. These included more thorough weapon searches, inspection of luggage, frisking and X-ray examination in search of bombs aboard aircrafts.

The government also introduced the use of Face-IT software at the Airport. That software can, used with surveillance cameras, recognise wanted individuals filmed by the camera. Permission from the Data Protection Authority is needed for the use of this equipment in Iceland, and the matter is currently under examination. Opinion is sharply divided on the use of that equipment, which critics say entails a risk of misuse. They argue that the spread and use of this technology is opposed to the principal of individual privacy and can rapidly lead to a "Big Brother is watching you" situation. On the other hand it is clear that this technology can be of great benefit in the search for criminals and wanted persons, but naturally it is important that strict rules be set on which types of data may be included in the database.

b) The government has initiated work on legislative amendments against terrorism. These may include bringing the criteria for the full commission of offences of this type into line with that of international conventions on terrorism; in most cases the criteria in such conventions are considerably stricter than that of the current Icelandic Penal Code.

Proposals for extensive authorisations for the police to engage on personal surveillance of any type, including telephone tappings and the monitoring of e-mail and other communication on the Internet, without first obtaining a court order have however not been met with general support.

In connection to this work, the National Commissioner of the Icelandic Police, called on financial institutions to apply particularly strict measures against money laundering in order to prevent the financing of terrorist acts.

c) In Iceland it has generally been regarded as vital to have a reliable civil defence system to meet the challenges posed by nature – such as avalanches, volcanic eruptions, earthquakes, floods etc. Now the focus of attention has changed and the concept of the term "civil defence" has been broadened to accommodate responses to attacks of various types, including those employing biological and toxic weapons.

A certain amount of funding was allocated for the purchase of equipment to prepare Icelandic hospitals to deal with the threat of terrorism. Measures taken include the establishment of a special laboratory which is probably the only one of its type in Europe with regard to the number of specimens of dangerous substances it can accept for analysis simultaneously.

d) The ministers of health of the Nordic countries have held some meetings to co-ordinate measures to prepare their health services to deal with the consequences of possible attacks using biological, chemical or atomic weapons. It was agreed the Nordic countries would collaborate and assist each other if such weapons were used by terrorists in the Nordic countries.

I have now given a very brief account of the main actions taken by Icelandic authorities due to the event of September 11th 2001. Many parties have proposed more radical actions, such as greater personal surveillance. Some, for example, have considered it natural to use a new surveillance technology developed by the US company Applied Digital. This technology includes the use of "personal identity ship", the size of a grain of rice, and placing it under a person's skin, so enabling all his or her movements to be monitored by means of surveillance satellite.

Obviously it is possible to use highly developed technology for various good purposes, e.g. to prevent kidnapping or to help rescue workers locate injured of missing persons. It could also open the way to maintaining virtually foolproof security in places where a high degree of reliable access control is necessary, for example at airports and in atomic power plants.

However, the dangerous side of such surveillance is also obvious, as it can be used to curtail the freedom of the ordinary citizen. New technology tends to be invented and introduced for purposes that everyone agrees are for the good, but it should always be asked what it could be used for the future, and how certain we can be if being able to prevent abuse.

Naturally, we must ensure the legislation meets the needs of the present day. It may be necessary to give the police wider powers, which may result in an abridgement of the individual's privacy of freedom of movement. On the other hand, all such measures must be designed to meet the particular threats they are designed to combat, and they must be in proportion to the dangers involved.

There are dangers inherent in legislative changes that are made under the pressure of public opinion demanding that something radical be done. Even though such legislation contains a "sunset provision", by which it is to be repealed on a certain date, there is always the danger that it will prove difficult to repeal when the time comes. There is always the danger that legislation of this type will go further than necessary, and in the present context there is a likelihood that foreigners will find themselves in a difficult position, that privacy in telecommunications will be invaded and that the basic principles regarding the protection of personal data will be abandoned.

My conclusion is that the greatest danger lies in giving in to the intentions of the terrorists. We must not sacrifice our long-term goals in the area of human rights, which include the privacy of the individual, for short-term security.

Ireland

To date in Ireland no special measures were introduced which impacted on Data Protection. However to implement developments at European Union level the government is preparing legislation to cover such matters as a common arrest warrant, mutual assistance in criminal matters, joint European investigation teams and cross border crime . In line with normal procedures the Office of the Data Protection Commissioner will be requested to give observations when the draft legislation is finalised and before it is published. In addition the whole question of retention of traffic data is also being reviewed in line with responsibilities under EU directives.

Isle of Man

REPORT ON THE IMPACT OF 11 SEPTEMBER 2001

1. Anti-Terrorism and Crime Bill 2002

   Comments upon the draft will were sought from interested parties earlier this year. It is envisaged that the Bill will come into force in the Spring of 2003.

   The Bill reforms and extends previous counter-terrorist legislation. The previous legislation concerned is:

- The Prevention of Terrorism Act 1990 ("the PTA")
- The Prevention of Terrorism (Amendment) Act 1992

   The Bill is based upon the Terrorism Act 2000 (of the UK Parliament) and some of the provisions of the Anti-Terrorism, Crime and Security Act 2001 (of the UK Parliament). The Bill repeals the PTA and re-enacts those of its provisions which remain necessary, with a number of modifications. The previous counter-terrorist legislation was originally designed in response to terrorism connected with the affairs of Northern Ireland and some of its provisions have subsequently been extended to certain categories of international terrorism. It did not apply to any other domestic terrorism. Under the Bill these restrictions are lifted, so that counter-terrorist measures are to be applicable to all forms of terrorism: Irish, international and domestic.

   Although this Bill contains extensive disclosure provisions it is my view that they are not disproportionate in terms of those permitted by human rights and data protection conventions, given the requirements in a democratic society for the safety of its citizens and the protection of their property.

2. The Terrorism (United Nations Measures) (Isle of Man) Order 2001

   This Order gives effect to UN Security Council Resolution 1363 (2001) in the Island. It provides that noone should facilitate the providing of funds to any entity and/or person involved in terrorism or facilitating terrorism. The Order makes it an offence to provide such funds. It also makes it an offence to not report to the authorities when there are reasonable grounds for suspecting that funds of any customer or client are being, or may be, used for the purpose of facilitating terrorism.

   Orders which give effect in the Island to the UN and EU instruments also provide the Isle of Man Treasury with powers to obtain information, carry out enquiries, issue licences and permissions to release funds, and to require institutions to freeze the funds of entities and/or persons. The Treasury has appointed its Customs and Excise Division to act for it in enforcing financial sanctions. In exercising these powers Customs and Excise has applied financial sanctions against Afghanistan, the Taliban and Osama Bin Laden and issued a list of persons whose accounts should be frozen.

Jersey

POST SEPTEMBER 11th – JERSEY SUMMARY

One of the most immediate and overt responses by Jersey to the terrorist attacks has been an increased uniformed presence at the Island's Airport. There has also been a significant rise in security checks being carried out by plain clothes officers monitoring passengers passing though the Island.

In the aftermath of the attacks, there was speculation about where the terrorist money was hidden and even some suggestions, quoted in the national press, that off-shore finance centres such as the Channel Islands were terrorist money factories.

The Jersey Government and finance industry (that handles funds of over £107 billion, and bank deposits of over £135 billion) were quick to respond and resources diverted from other key areas into the changes that have been made in implementing a revised Terrorism Law, a Crime and Security Law as well as a review of the implementation of UN Security Council Resolutions.

The Joint Financial Crime Unit (JFCU) – staffed by Police and Customs – received additional resources and now has 15 full time personnel.

The finance industry and the Police continue to view Suspicious Transaction Reports (STR's) as an effective tool. Legislation designed to prevent the laundering of money associated with crime, drugs and terrorism through the Island requires local financiers to look out for strange or unaccounted movements of funds and submit STR's to JFCU for investigation. In 2001, a total of 972 STR's were submitted which is an increase of 54% on 2000.

During 2001, the States of Jersey Police handled over 50 external enquiries a month including requests for assistance from the United Kingdom and countries as far afield as Mauritius. Work is also continuing on the Police Procedures and Criminal Evidence Law and Regulation of Investigatory Powers.

Another topic that is being seriously considered in Jersey is the introduction of resident/identity cards although there are no imminent plans for their introduction prior to full consideration and debate on the surrounding issues.

Netherlands

The first reaction of the Dutch government (Prime Minister Wim Kok) was very moderate. Mr. Kok (social-democrat) was upset by the terrible event, but he also stressed the importance of a reaction with dignity: "let's keep upright the values of democracy and human rights!"

In October the government presented a plan for action against terrorism consisting of 43 proposals which aimed at:
- improved cooperation between police and intelligence services, including the exchange of information.
- extension of security measures at the borders, airports etc.

3. From a point of view of data protection the following proposals were interesting:
- acceleration of a draft bill for interception of telecommunication;
- introduction of biometric data on travel documents;
- temporary obligation for identification in situations where there is a real and imminent danger for a terrorist attack.

Many proposals focussed on getting more grip on the financial sector for law enforcement agencies. It is our impression that such plans already existed, but that the Minister of Finance waited for the right moment to compel the financial sector to cooperate with these agencies. One of the proposals was a legal obligation for banks and insurance companies to provide the police with information about their clients.

The first reaction of the heads of police in the autumn of 2001 was also very moderate: no need for more legal powers to combat terrorism.

The political climate really changed in the last months before the general elections on May 15th. A newcomer, right winger Pim Fortuyn drew much attention by stressing the importance of a more adequate policy in combating crime and illegal immigrants and constraining the number of asylum seekers. The existing political parties joined this movement or got confused by the enormous growing popularity of Pim Fortuyn. Then 10 days before the elections, he was murdered, as it seems, by an environmentalist. His party (LPF) became the second party, even without a leader. The elections also brought a victory for the Christian Democrats.

The new government started on July 22th with the following statement on privacy protection: "More generally spoken, we aim at restoring the balance between the protection of society and the (potential) victims against the rights of (potential) criminals and the protection of their privacy." Concrete proposals are the implementation of a general obligation for identification, more powers for the police for searching vehicles, using DNA techniques on a larger scale and more matching of data files for criminal investigation.

Conclusion. The Dutch Data Protection Authority is confronted with a shift of politics as a direct result of the general elections. This reflects a broad change in the attitude of the public towards issues like safety for the citizens, the combat against crime and terrorism, and the right to privacy. There is much to do to make clear that feeling safe and having a certain degree of privacy are interconnected. An overkill of measures by law enforcement agencies only gives a fake feeling of safety, and from the point of view of privacy, puts a great burden on the citizens for which a convincing legitimation is lacking.

New Zealand

New Zealand Report to 24th International Conference of Data Protection and Privacy Commissioners, Cardiff, 9 September 2002
Impact of 11 September 2001

The Terrorism (Bombings and Financing) Bill was introduced into the New Zealand Parliament in April 2001, before the events in question, to implement two international conventions. Following 11 September the select committee studying the bill proposed a number of amendments to give effect to UN Security Council Resolution 1373. The Privacy Commissioner made submissions on some of the changes and expressed concerns at denying accused persons access to certain classified security information which might be necessary for their defence. The bill had not been enacted when Parliament was prorogued for a General Election to be held on 27 July.

The United Nations Sanctions (Terrorism Suppression and Afghanistan Measures) Regulations 2001 were issued on 26 November pursuant to the United Nations Act 1946. It takes measures against the Taliban, Usama bin Laden and Al-Qaida including banning collecting or providing funds, dealing with property, recruitment, participation or providing certain services. It also creates a duty to report suspicions relating to property. These special measures will be replaced, in due course, by a more general regime once the Terrorism (Bombings and Financing) Bill has been enacted.

The Transnational Organised Crime Bill was introduced in February 2002 and enacted in July making a variety of amendments to Crimes, Extradition, Immigration, Mutual Assistance in Criminal Matters, Passports and Proceeds of Crime Acts. The bill implements the UN Convention against Transnational Organised Crime and its protocols on the smuggling of migrants and trafficking in persons. Extraterritorial jurisdiction is taken for some offences. One area with data protection implications is provision for disclosure of information to overseas agencies. Increased employer checks of employee immigration status is also anticipated. A controversial feature, challenged before the courts, has been the introduction of routine detention of asylum seekers.

Beyond the legislature and courts, the level of security at NZ airports was immediately stepped up with introduction of x-ray screening on domestic flights within 48-hours of 11 September. The Government has established this as a permanent security feature. The Government has also deployed NZ troops in Afghanistan.

A session on "Terrorism, National Security and Privacy: Continuing to Strike a Balance" was included in the 3rd Asia Pacific Forum on Privacy and Data Protection hosted by the Privacy Commissioner in Auckland in March. Presentations from Canada, Ireland and New Zealand were given.

B H Slane
New Zealand Privacy Commissioner

Norway

The impact of September 11th in Norway

White Paper No. 17 to Stortinget (The Norwegian Parliament) (2001-2002) on the Safety and Security of Society was presented on April 5th 2002 by The Norwegian Ministry of Justice and Police. The basis for the report is partly a result of the terror attacks on September 11th 2001. The White Paper is a comprehensive statement on the government's proposals to reduce the vulnerability of modern society and how to increase safety and security in the years to come, and will form the basis for the government's process of initiating measures.

On page 2 in the summery:
"The terror attacks on September 11th 2001 demonstrate the vulnerability of modern society, and that such incidents in times of peace can cause just as much damage as acts of war. This change in the situation of threats and hazards where the society must be capable of dealing with variety of challenges in addition to military threats, will be taken into account when arranging and giving priority to today's work on security and safety. As a result of the terror attacks, it has been considered necessary to increase the national safety and security, particularly within the Police Security Service, the Civil Defence and the emergency planning within the Health sector.".

The White Paper stresses the importance of improving the emergency planning in several sectors. In order to meet the threats against information and communication technology a Centre of Information Security will be established, the plans for preparedness in case of the arrival of large numbers of refugees and people seeking political asylum are being reviewed, measures against organised crime are being assessed and the role of the Police force is thoroughly discussed. All these measures will most likely demand implementation of several new provisions and regulations. These provisions and regulations might be of great impact on privacy issues.

The ministry of Justice has proposed an addition to the Criminal Act, where the act of terror is made punishable. The proposal will, if approved, establish comprehensive alterations within the criminal law. The addition comprises legal provisions regulating a possible punishment of six years imprisonment for planning and preparing terror actions. Enforcement of such a provision might entail extraordinary methods of investigation such as technical tracking and different forms of communication control systems, methods that will threaten the individual's right to privacy.

Økokrim (The National Authority for Investigation and Prosecution of Economic and Environmental Crime in Norway) argue that traffic data from the telecommunication systems should be retained in a data warehouse controlled by The National Computer Crime Centre after the original purpose is fulfilled, in case of crime investigation. Retention for one year has been suggested, but there is currently no proposal from The ministry of Justice.

After the terror attacks on September 11th 2001 The Data Inspectorate has received several complaints on The Embassy of Israel from the neighbours. The complaints concern video surveillance of the neighbours' properties. There is currently a dialogue between The Data Inspectorate and The Embassy of Israel.

In the annual report The Data Inspectorate states that the debate after September 11th has been moderate and objective concerning measures to prevent terror acts.

Spain

According to your kind request I am pleased to inform you about the impact in Spain of the 11th of September events.

First of all, it must be mentioned that not great changes has been made until very recent dates on the Spanish legal framework as regards data protection due to the September 11 events for Spanish Law Enforcement agencies deemed it adequate in order to fulfil their tasks.

Nevertheless, the situation has changed recently but mainly due to the negotiations in the Council of the UE of the new Directive on Privacy in the Telecommunications Sector and the movements towards a more harmonised approach to retention of traffic data. In this situation, the discussion in the Senate (Upper House of the Parliament) of the new Act transposing into Spanish Law Directive 2000/31/EC (Electronic Commerce) gave way to the inclusion of a new article dealing with systematic retention of traffic data only for Law Enforcement Purposes for a maximum period of a year.

The final wording of the article after the Agencia de Protección de Datos issued its mandatory opinion reflected to some extent the concerns and remarks it has made. The main changes referred to the narrowing of the scope of the data to be kept (only those necessary to find the terminal equipment used for transmitting the information), the explicit inclusion of a paragraph establishing that retention in no case can affect the secret of telecommunications, the impossibility to use the stored traffic data for a purpose different to those mentioned in our opinion, the adoption of stringent security measures to avoid unauthorised access to the data and the establishment of the obligation to respect the rules present in the data protection legislation when Law Enforcement agencies gain access to the information.

Besides, there is now a Bill being discussed in Congress (Lower House of the Parliament) on the Prevention and blocking of funding of terrorism. In its preamble, the bill makes an explicit reference to the September 11 events as well as to some United Nations resolutions and European Union agreements in base of which some measures aimed to prevent economical transactions made by or on behalf of terrorists are drafted. It sets up a Monitoring Commission with powers to gather certain information from financial entities and block economic assets and transactions in the concrete cases specified in the Bill. The Bill establishes the applicability of the data protection legislation and the supervision of the Agencia de Protección de Datos to the personal data processing operations carried out by the Monitoring Commission. Besides, apart from the supervision task regarding data protection entrusted to our office, there is a judicial supervision of the decisions taken by the Monitoring Commission.

Juan Manuel Fernández López
Director

Sweden

Report for the Cardiff World Conference on the impact of September 11th

Security legislation and citizens' rights on data protection

In March, the Swedish Government presented two bills to the Parliament concerning the combating of terrorism. One bill referred to the International Convention of the United Nations for the Suppression of the Financing of Terrorism and Sweden's accession to this Convention. The other bill referred to Sweden's approval of the framework decision of the EU Council on combating of terrorism. On May 29th the Parliament decided to adopt both bills.

As to Sweden's accession to the UN Convention, the Government proposed a new Act on sanctions for the financing of especially serious crime in certain cases. It will be punishable to collect, provide or receive money or other funds with the intention that they should be used for an act which constitutes an offence within the scope of the Convention. Also attempts will be punishable. The specific Act implementing the UN Convention entered into force on 1st July.

The second bill regards the framework decision of the EU Council on combating of terrorism. This decision contains provisions as to what acts shall be deemed to constitute terrorist crimes in the national legislations of the member States as well as what sanctions that shall apply. No amendments are actually presented in the bill. However, the Government outlines what amendments of law that will be necessary in order to comply with the framework decision. There is a need for further analysis before a proposal of a new Act or proposals for amendments of existing Acts can be presented. The Government intends to introduce a bill with proposals for amendments in the autumn.

In the autumn of 2001 legislative work was also being prepared in Sweden as to freezing of funds and financial assets. At the same time a Council Regulation was being elaborated within the EU. The Council Regulation on specific restrictive measures directed against certain persons and entities was adopted on December 27th 2001. There is an annex to the regulation with a list of persons against whom restrictive measures are to be directed. It is based on a list from the UN. Now and then changes are made in the list which cause a lot of work for banks and insurance companies. The banks must compare the changed list with the old one and this work requires quite a lot of personnel resources.

Quite a few practical problems have arisen and there is a discussion going on within the Swedish Bankers' Association and the Financial Supervisory Board on how to handle, for instance, repayment by instalments and interests in connection with the freezing of funds.

In Sweden six financial institutions have frozen funds, insurances and certain financial services for three individuals – Swedish citizens of Somalian origin – and at least two entities. There are also restrictions regarding these persons' right to travel (based on a UN Resolution).

There is also special legislation regarding sanctions, the Sanctions Act of 1996, containing provisions of sanctions if, for instance, a bank does not freeze funds according to what has been set forth in an EC Regulation.

Finally, the Government presented a bill to the Parliament concerning the framework decision of the EU on the European arrest warrant; the bill was adopted on 22 May. This concerns the extradition of Swedish citizens under certain circumstances to other EU-countries for the purpose of taking legal proceedings against a certain individual. There are no proposals for amendments of law presented in the bill. The Government intends to present a new bill in the spring of 2003 with proposals for amendments. According to existing legislation Swedish citizens can only be extradited to other Nordic countries.

Switzerland

The impact of 11 September 2001 on data protection in Switzerland

The tragic events of 11 September 2001, closely followed by the massacre of 21 September 2001 in the chambers of the Cantonal Parliament in Zug have changed the relationship between public security and data protection. At the centre of the debate there emerges the question as to what extent data protection can be guaranteed when confronted with the needs of public security. Since 11 September, a major debate has begun on security and the guarantee of the rights and freedoms of individuals in relation to the handling of personal data.

The Federal Data Protection Commissioner immediately stressed the necessity of adopting a cautious and responsible attitude. It is of fundamental importance to ensuring a balance between the security of the public and property and the protection of data. It should not be forgotten that extreme restrictions on fundamental rights affect our freedoms permanently and irreversibly undermine democracy, thus playing into the hands of the terrorists. Furthermore, it should be remembered that the security services and the prosecution authorities had extensive powers in relation to the handling of personal data before these events took place. This being the case, the widespread and hasty restriction of the application of the regulations for the protection of data is not required. If security measures have to be introduced, they have to be necessary and have to be discussed beforehand. In every case, it must be ensured that additional security measures do not encroach on the private domain in a disproportionate manner. Such measures must be made subject to democratic control, notably by the data protection authorities.

To date, despite certain external pressures and numerous parliamentary moves, September 11 has not led to the adoption of disproportionate measures. The Federal Council (government) has extended the list of organisations that are potentially dangerous to internal security and that are subject to surveillance by internal security agencies. On 7 November 2001, it passed a decree in implementation of the Federal Act of 21 March 1997 on measures to safeguard internal security (ASIS) that provided for the extension of the duty to provide information and of the right of federal and cantonal authorities and offices to pass on information to the internal security services. The Federal Council, on the other hand, rejected the introduction from 1 January 2003 of biometrical data on passports and identity cards.

The Federal Council has proposed the rapid ratification of the Council of Europe convention on cyber crime. It is also proposing the ratification of two United Nations conventions on combating terrorism and the introduction of new criminal offences in the fight against terrorism These new offences have been the object of vehement criticism from criminal law experts, who consider them to be ineffective.

A project to revise the Federal Aliens Act is planning the introduction of a provision permitting the use of video surveillance or recognition systems, and in particular a facial recognition system. The provision as proposed to Parliament would permit not only the identification of persons who are not allowed to enter Swiss territory, but also the gathering of data for the purpose of combating terrorism. A pilot project will be set up this summer at Zurich-Kloten airport.

Lastly, the Federal Council is looking into further measures in the field of internal security and is shortly expected to propose the revision of the law on measures to safeguard internal security. Following our intervention, the Federal Office of Justice and Police will be required beforehand to submit a report giving its overall view on all the measures envisaged.

Thailand

Thai citizens ' privacy right are constitutionally guaranteed. The constitution of kingdom of Thailand 1997 section 34 said

"A persons family rights , dignity, reputation or the right of privacy shall be protected. The assertion or circulation of a statement or picture in any manner whatsoever to the public, which violates or affects a person's family rights, dignity, reputation or the right of privacy , shall not be made expect for the case which is beneficial to the public"

In addition the only Official Information Act 1997 has also guaranteed not only the privacy right but also the freedom of information, section 15 said

" A state agency or state official may issue an order prohibiting the disclosure of official information falling under any of the following descriptions, having regard to the performance of duties of the State agency under the law, public interest and the interests of the private individuals concerned:

(5) a medical report or personal information the disclosure of which will unreasonably encroach upon the right of privacy;

Still, Thailand and many countries are a long way from having a genuinely freedom of information and privacy rights. Wire-tapping cases are reported by mass media. In Thailand , it is still believed that privacy rights are violated by state agencies concerned national security and sometime beyond the national security.

According to the new bureaucratic reform bill, the new special investigation department(we call F.B.I.) will be set up under the ministry of Justice in order to handle and tackle the special criminal case. The SID will have authority to do wire-tapping, opening the personal letter or mailing.

Thailand is a member of the ASEAN group. Thailand also has signed a sweeping treaty with Southeast Asian nations and the United States aimed at making the region against terrorism

The United Kingdom

Challenges arising from the events of 11th September 2001
The Information Commissioner, United Kingdom

The terrorist atrocities in New York, Washington and Pennsylvania on 11 September last year sent shock waves around the world. The United Kingdom's data protection environment has not been immune to this and the aftershocks continue to be felt. The UK Government has been galvanised into action to try to ensure that similar terrorist atrocities could never re-occur. One of the main thrusts has been directed towards legislative initiatives, with potentially far reaching consequences. These initiatives have lead to a noticeable shift in the balance between respect for an individual's private life and the needs of society to protect itself against such criminal actions. However, although this shift has occurred in the name of terrorism, the measures deployed often go much further into areas of more usual criminality.

In the United Kingdom, the most notable legislative response undertaken by Government was the passage of the Anti-Terrorism, Crime and Security Act 2001. This includes significant features such as removing barriers to information sharing between official bodies and also providing mechanisms to extend the period of retention of communication data beyond the communication service providers own commercial needs. The provisions contained in the legislation have a much wider effect than simply putting in place necessary measures to deal with the terrorist threat.

The provisions relating to the retention of communications data by communication service providers are of continuing concern. When the legislation was originally published we expressed concern over the "voluntary" mechanisms to be used to achieve extended retention and also the breadth of purposes for which this retained information could be used. Although during the passage of the legislation there were welcome changes, such as requiring consultation with the Information Commissioner on the proposed Code of Practice and limiting the continued retention to matters in relation to national security, worryingly the basis on which law enforcement bodies can have access to this communications data is not similarly restricted. In effect, the communications data retained by communication service providers for the purpose of safeguarding national security can be accessed for any of the wider law enforcement activities using the provisions of the Regulation of Investigatory Powers Act 2000. These wider requirements to disclose encompass not just general criminality, but also matters relating to public health and tax collection. The potential for the accessing of information retained for safeguarding national security for these much wider purposes is of particular concern.

Proposals have also been put forward by the Government to amend existing legislative provisions relating to money laundering, in an effort to address concerns about the financing of terrorist organisations and the wider criminal fraternity. The latest proposals, if accepted by Parliament, will result in a compulsion on all money remitters to include the name, address and any account details on all money transfers sent from the UK, both abroad and within the UK. We are concerned that this is a disproportionate response as it will affect the innocent majority with increased risks of unwarranted intrusion on their privacy and put the security of this information at risk.