Privacy and Human Rights 2002: An Extract of the International Survey of Privacy Laws and Developments

ELECTRONIC PRIVACY INFORMATION CENTER
AND PRIVACY INTERNATIONAL*

Global political conjunctures exhibit how Washington's war against terrorism post 9/11 can easily translate into a war against freedom and privacy. The Internet, as a medium of political and private communication, is being subjected to state controls which impinge on the civil liberties of Netizens. It gradually becomes an instrument of oppression rather than of freedom and openness. The 9/11 event has compelled nation-states to re-examine their security mechanisms. Countries like New Zealand, Australia, France, Germany, South Africa, Canada, India, United Kingdom, Zimbabwe, USA and the Philippines have instituted legal and social strictures as protection to foreign aggression. These efforts are supportive of the Bush government's crusade to increase communication surveillance of transactional-local data and communication technologies, weaken data protection statutes, increase data sharing and profile identification and control data traffic in the Web. Concomitantly, supranational bodies like the Council of Europe, G-8 and the European Union have ventured on the formulation of legal and economic frameworks in averting the increasing number of cybercrimes.

Threats to Privacy

Even with the adoption of legal and other protections, violations of privacy remain a concern. In many countries, laws have not kept up with the technology, leaving significant gaps in protections. In other countries, law enforcement and intelligence agencies have been given significant exemptions. Without adequate oversight and enforcement, the mere presence of a law may not provide adequate protection. Finally, with recent transformations to data protection regimes, further gaps, exemptions, and inadequacies are arising.

The Response to September 11, 2001

It may take some years to fully evaluate the effects of the 11 September 2001 World Trade Center bombing on privacy and civil liberties.

*The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. Privacy International (PI) is a human rights group formed in 1990 as a watchdog on surveillance by governments and corporations. PI is based in London, England, and has an office in Washington, D.C. An electronic version of this report and updates is available from the Privacy International web page at http://www.privacyinternational.org/.

Shortly after the events of that day, previous proposals were re-introduced, and new policies with similar objectives were drafted to extend police surveillance authority.

The policy changes were not limited to the United States, as a large number of countries responded to the threat of terrorism. The country reports in this survey outline, in more detail, the many legislative shifts that took place around the world.

It was a time of fear, flux and uncertainty. The United Nations responded with Resolution 1368 calling on increased cooperation between countries to prevent and suppress terrorism.[1] North Atlantic Treaty Organization (NATO) invoked Article 5, claiming an attack on any NATO member country is an attack on all of NATO; legislatures responded accordingly. The Council of Europe condemned the attacks, called for solidarity, and also called for increased cooperation in criminal matters.[2] Later the Council of Europe Parliamentary Assembly called on countries to ratify conventions combating terrorism, lift any reservations in these agreements, extend the mandate of police working groups to include "terrorist messages and the decoding thereof."[3] The European Union responded similarly, pushing for a European arrest warrant, common legislative frameworks for terrorism, increasing intelligence and police cooperation, freezing assets and ensuring passage of the Money Laundering Directive.[4] The OECD furthered its support for the Financial Action Task Force on Money Laundering and, along with the G-7[5] and the European Commission, called for the extension of its mandate to combat terrorist financing.[6] These calls for international cooperation were perceived by many as impetus to create new laws.

The European Commission considered requiring every member state of the European Union to make cyber-attacks punishable as a terrorist offence. New Zealand minimized public consultation on a proposed law to freeze the financial assets of suspected terrorists because the government felt it was bound by United Nations Security Council resolutions. France expanded police powers to search private property without warrants. Germany reduced authorization restraints on interception of communications, and increased data sharing between law enforcement and national security agencies.

Australia and Canada both introduced laws to redefine *terrorist activity* and to grant powers of surveillance to national security agencies (*ASIO* and *CSIS* respectively) for domestic purposes if terrorist activity or a terrorist affiliation is suspected. India passed a law to allow authorities to detain suspects without trial, conduct increased wiretapping, and seize funds and property. The United Kingdom passed a law permitting the retention of data for law enforcement purposes in contravention to existing data protection rules. The United States passed a number of laws, including the USA-PATRIOT Act, which increases surveillance powers and minimizes oversight and due process requirements.

The above list of international and national initiatives is not exhaustive. New policies are being proposed every week with the goal of investigating, preventing, and suppressing terrorist activity. However, within this deluge of new policy proposals, a number of trends may be identified.

Increased Communications Surveillance and Search and Seizure Powers

Almost every country that changed its laws to reflect the environment following September 2001 increased the ability of law enforcement and national security agencies to perform interception of communications, and transformed the powers of search and seizure, and an increase in the type of data that can be accessed.

The novelty in these initiatives tends to arise in the reduced authorization requirements and oversight. This includes initiatives to weaken due process requirements; as occurred in Canada where the first anti-terrorism bill proposed that law enforcement agencies will no longer be required to justify the need for the wiretap. That is, in existing law, the judge authorizing the interception would need to be satisfied that "other investigative procedures have been tried and have failed, other investigative procedures are unlikely to succeed or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures."[7] In the law, an exception is established for all offences that fall under the broad category of "terrorist activity." Other parts of the law allow for interception authorization by the Minister of Defence instead of requiring judicial authorization.

There is also a general increase in the breadth of application of these powers, by incorporating and including new technologies and

communications infrastructures, permitting additional government agencies to use these powers, and formalize roving powers. The USA-PATRIOT Act codified the use of Carnivore-style Internet surveillance technology, granting access to sensitive traffic data with only a court order rather than a judicial warrant. Moreover, the reporting regime in the United States was weakened with amendments to the Foreign Intelligence Surveillance Act so that fewer warrants would have to be requested and reported because the expiration time period was increased, and 'generic' orders could be requested allowing one warrant to be served on multiple service providers.

Attempts to differentiate the authorization and oversight requirements based on the communications-technology also occurred. The Australian government proposed in its Telecommunications Interception Legislation Amendment Bill 2002 to grant powers to intercept and read e-mail, short messaging system (SMS) and voice mail messages without a warrant because these communications were considered access to 'stored' data rather than 'intercepted' in real-time. This proposed act was rejected in the Senate in June 2002;[8] however, the Government claims that it "remains of the view that the approach adopted in the bill with respect to stored information is appropriate. However, to avoid holding up this important package of legislation, the government has agreed to remove these provisions from the bill and to deal with the issue at a later date."[9]

Weakening of Data Protection Regimes

In 2000, the United Kingdom proposed a policy to require the retention of communications traffic data for up to 7 years by a central government authority.[10] While the proposal faced significant resistance in the public discourse at that time, in December 2001 a similar policy was introduced and passed under the United Kingdom's anti-terrorism law in response to the events of September 2001. The new European Union directive on data protection in electronic services also supports the creation of such data retention laws within the European community and is consistent with international pressure to weaken data protection. In October 2001, President Bush sent a letter to the President of the European Commission requesting that the European Union "[c]onsider data protection issues in the context of law enforcement and counterterrorism imperatives," and as a result to "[r]evise draft privacy directives that call for mandatory destruction to permit the retention of critical data for a reasonable period."[11] Building from previously articulated

concerns that "[d]ata protection procedures in the sharing of law enforcement information must be formulated in ways that do not undercut international cooperation,"[12] the United States Department of Justice submitted a number of recommendations to the European Commission working group on cybercrime, including the recommendation that,

> Any data protection regime should strike an appropriate balance between the protection of personal privacy, the legitimate needs of service providers to secure their networks and prevent fraud, and the promotion of public safety.[13]

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

> Ensure data protection legislation, as implemented, takes into account public safety and other social values, in particular by allowing retention and preservation of data important for network security requirements or law enforcement investigations or prosecutions, and particularly with respect to the Internet and other emerging technologies.[14]

Further discussion regarding the reduction of the protections of privacy afforded by data protection law will likely arise in September when the European Commission continues discussion of the implementation of the 1995 directive (95/46/EC).

Individuals and citizens are at the same time losing subject access rights under data protection and freedom of information regimes. In the interests of critical infrastructure protection, access to information is being reduced, limiting government accountability. Meanwhile, in order to protect sensitive investigative and intelligence data, subject access requests are restricted as some data banks are being exempted from both data protection and freedom of information laws.

Increased Data Sharing

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

There are significant shifts in the policies and practices in the United States with changes to the Attorney General Guidelines regulating the actions and capabilities of the Department of Justice and FBI, increased sharing of information between the FBI and CIA supported by the USA-PATRIOT Act, and proposed policies to increase sharing with local law enforcement agencies. The United States is not alone in introducing such policies. The United Kingdom is proposing "joined-up government" within its consultation paper on modernizing government and public services to create "data-sharing gateways" and provide "seamless" services.[15] It also tried unsuccessfully to allow practically any government agency to gain access to the traffic data of individuals under the Regulation of Investigatory Powers Act, including local councils and parishes.[16]

The increased flow of data is also coming from the private sector. The United Kingdom and Canada proposed laws to grant law enforcement agencies access to travelers' information. The United Kingdom Home Office has recommended that it gain access to information from every passenger before international flights.[17] The Canadian policy proposes to grant both the federal law enforcement and the intelligence agencies access to air passenger information, regardless of domestic or international travel, and to match this data with other personal information,[18] for a wide number of purposes and investigations, not limited only to terrorism.[19]

Similarly, the European Union is considering granting Europol access to the Schengen Information System, including privileges to change the information held on travelers.[20] Germany has recommended to the European Union the creation of a database of "known trouble-makers," to be used "for criminal prosecution purposes and in order to avert dangers constitute a proper and necessary tool in the fight against international terrorism. However, in view of the fact that members and supporters of terrorist groups are known to roam across Europe, the measure would be much more effective if it were applied by all European Union Member States."

Data sharing between financial institutions and with government agencies has also increased. New money laundering agreements and regulations have been introduced to increase surveillance of transactions, and even expanded to include hedge funds and money transfer firms.[21] Donations to charities are receiving further scrutiny as both the charities and the donors are monitored to investigate links with terrorist groups.[22]

Some financial institutions are also sharing personal information between themselves in order to minimize risk of clients being terrorists, or "undesirables".[23]

Increased Profiling and Identification

Following from data sharing, there are a number of proposals to create profiles or increase the existing profiles of individuals. This occurs in a number of ways; the most immediate appears to be the profile of travelers. There are proposals for a next generation computer-assisted passenger prescreening system that will bring in data from credit-reporting agencies and other companies,[24] and even previous flights and registries, set for data mining.[25] Other proposals include trusted-traveler programs involving biometrics in both the United States and Germany,[26] similar to schemes used at Ben Gurion Airport in Tel Aviv.[27] Some airports have also installed face-recognition technologies, while similar technologies are being implemented at national monuments, and even beaches.

In the longer term there are a number of proposals to increase profiling of citizens and non-citizens. These proposals are typically enhanced and complemented by national identification schemes, enhanced with biometrics. There was considerable discussion in the United States in introducing such a national ID card scheme but no formal policy was introduced. Meanwhile non-citizens may already be tracked at border entry points and as they move within the country. A system called Student and Exchange Visitor Information System keeps track of foreign students to ensure that they are still registered and maintains a log of their addresses.

The United Kingdom is proposing the implementation of 'entitlement cards' in an effort to deal with immigration and illegal work, identity theft, but also supported by the fight against terrorism. Similarly, Hong Kong is planning to introduce a biometric chip identity card to verify fingerprints to authenticate travelers into China.

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

Transactional and Location Data: Surveillance and New Communications Technologies

As new telecommunications technologies emerge, many countries are adapting existing surveillance laws to address the interception of networked and mobile communications. These updated laws pose new threats to privacy in many countries because the governments often simply apply old standards to new technologies without analyzing how the technology has changed the nature and sensitivity of the information. It is crucial for the protection of privacy and human rights that transactional data created by new technologies is given greater protection under law than traditional telephone calling records and other transactional information found in older systems.

In the traditional telephone system, transactional data usually takes the form of telephone numbers or telephone identifiers, the call metrics (e.g. length of call, time and date), countries involved, and types of services used. This data is usually collected and processed by telephone companies for billing and network efficiency (e.g. fault correction) purposes. While this data is stored by telephone companies, it is available to law enforcement authorities. Communications content, i.e. conversations, are not stored routinely. As a result, the obstacles to law enforcement access to this data were minimal: traffic data was available, legally less sensitive, and so accessible with lower authorization and oversight requirements. The content of communications was treated as more sensitive, and more invasive, and more difficult to collect, thus typically requiring greater authorization and oversight mechanisms.

Different communications infrastructures give rise to different forms of transactional data, however. When surfing the net, a user can visit dozens of sites in just a few minutes and reveal a great deal about their personal situation and interests. This can include medical, financial, social interests and other highly personal information. As the Council of Europe acknowledges in the Explanatory Report of the Convention on Cybercrime,

> The collection of this data may, in some situations, permit the compilation of a profile of a person's interests, associates and social context. Accordingly Parties should bear such considerations in mind when establishing the appropriate safeguards and legal prerequisites for undertaking such measures.[28]

The detailed and potentially sensitive nature of the data makes it more similar to content of communications than telephone records.

Similarly, location information generated by mobile communications infrastructure, such as mobile phones and mobile IP, is more sensitive than the mere location of a fixed telephony communication. Mobile communications location information can provide details of an individual's movements and activities and whom they have met with. This location information may be combined with other transactional information such as websites visited using the mobile device, individuals called, search engine requests; all used to create a considerable profile. This affects a wide variety of human rights beyond the right of privacy including the rights of free speech and assembly.

The level of legal protection afforded to other traffic data is similarly unclear. Policies generally treat all of this transactional data as 'traffic data'; this data then bears the protections afforded under the traditional telephone system. The United Kingdom in its Regulation of Investigatory Powers Act 2000 accepted, after an extensive debate, that there are varying levels of sensitivity to this data, and separates 'traffic data' (source and destination of a transaction used for routing within a network) from the more sensitive 'communications data' that includes URLs, domain names, etc. The latter requires greater authorization and oversight procedures. Not all countries have pursued this line of reasoning.

Previous United States policy differentiated between traffic data on cable and telephone communications. The Cable Act traditionally protected traffic data to a greater degree than telephone traffic data. Now that cable infrastructure is used for internet communications (which were previously used over telephone lines, and thus traditional laws applied), successive White House administrations worked to erase this distinction, finally succeeding with the USA-PATRIOT Act. Rather than deal with the specifics of digital communications media and services, the changes in United States law reduce the protections of traffic data for all communications to what had previously existed for telephone communications data. This was clearly intended, under the guise of technological neutrality. According to Attorney General Ashcroft:

> Agents will be directed to take advantage of new, technologically neutral standards for intelligence gathering. (...) Investigators will be

directed to pursue aggressively terrorists on the Internet. New authority in the legislation permits the use of devices that capture senders and receivers addresses associated with communications on the Internet.[29]

Retention of Traffic and Location Data[30]

On May 30, 2002, the European Parliament voted on the new European Union Telecommunications Privacy Directive.[31] In a remarkable reversal of their original opposition to data retention, the members voted to allow each European Union government to enact laws to retain the traffic and location data of all people using mobile phones, SMS, landline telephones, faxes, e-mails, chatrooms, the Internet, or any other electronic communication devices, to communicate. The new Directive reverses the 1997 Telecommunications Privacy Directive by explicitly allowing European Union countries to compel Internet service providers and telecommunications companies to record, index, and store their subscribers' communications data.[32] The data that can be retained includes all data generated by the conveyance of communications on an electronic communications network ("traffic data") as well as the data indicating the geographic position of a mobile phone user ("location data").[33] The contents of communications are not covered by the data retention measures. These requirements can be implemented for purposes varying from national security to criminal investigations and prevention, and prosecution of criminal offences, all without specific judicial authorization.

Although this data retention provision is supposed to constitute an exception to the general regime of data protection established by the directive, the ability of governments to compel Internet service providers and telecommunications companies to store all data about all of their subscribers can hardly be construed as an exception to be narrowly interpreted. The practical result is that all users of new communications technologies are now considered worthy of scrutiny and surveillance in a generalized and preventive fashion for periods of time that States' legislatures or governments have the discretion to determine. Furthermore, because of the cross-border nature of Internet communications, this Directive is likely to have negative repercussions for citizens of other countries. There is a significant risk that non-European Union law enforcement agencies will seek data held in Europe that it can not obtain at home, either because it was not retained or because their national law would not permit this kind of access.

During the debates on the Directive, many members of the European Parliament, and the European Union privacy commissioners consistently opposed data retention, arguing that, these policies are in contravention of data protection practices of deletion of data once it is no longer required for the purpose for which it was collected; and also in contravention of proportionality principles in accordance with constitutional laws and jurisprudence. Similarly, the Global Internet Liberty Campaign, a coalition of 60 civil liberties groups organized a campaign and drafted an open letter to oppose data retention. The letter was sent to all European Parliament members and heads of European Union institutions after more than 16,000 individuals from 73 countries endorsed it in less than a week.[34] The letter asserted that data retention (for reasons other than billing purposes) is contrary to well-established international human rights conventions and case law.

While a few other countries have already established data retention schemes (Belgium, France, Spain and the United Kingdom) the implementation phase of the Directive's data retention provision may be bumpy in other Member States. The Directive may be seen as being in conflict with the constitutions of some European Union countries, with respect to fundamental rights such as the presumption of innocence, the right to privacy, the secrecy of communications, or freedom of expression.[35]

'Cybercrime': International Initiatives in Harmonizing Surveillance

A related effort for enhancing government control of the Internet and promoting surveillance is also being conducted in the name of preventing "cyber-crime," "information warfare" or protecting "critical infrastructures". Under these efforts, proposals to increase surveillance of the communications and activities of Internet users are being introduced as a way to prevent computer intruders from attacking systems and to stop other crimes such as intellectual property violations.

The lead bodies internationally are the Council of Europe and the G-8, while there has also been some activity within the European Union.[36] The United States has been active behind the scenes in developing and promoting these efforts.[37] After meeting behind closed doors for years, these organizations finally, in 2000, made public proposals that would

place restrictions on online privacy and anonymity in the name of preventing cybercrime.

Council of Europe

The Council of Europe is an intergovernmental organization formed in 1949 by West European countries. There are now 43 member countries. Its main role is "to strengthen democracy, human rights and the rule of law throughout its member states." Its description also notes that "it acts as a forum for examining a whole range of social problems, such as social exclusion, intolerance, the integration of migrants, the threat to private life posed by new technology, bioethical issues, terrorism, drug trafficking and criminal activities."

On 8 September 1995, the Council of Europe approved a recommendation to enhance law enforcement access to computers in member states. The Recommendation of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information states:

> Subject to legal privileges or protection, investigating authorities should have the power to order persons who have data in a computer system under their control to provide all necessary information to enable access to a computer system and the data therein. Criminal procedure law should ensure that a similar order can be given to other persons who have knowledge about the functioning of the computer system or measures applied to secure the data therein.
>
> Specific obligations should be imposed on operators of public and private networks that offer telecommunications services to the public to avail themselves of all necessary technical measures that enable the interception of telecommunications by the investigating authorities.
>
> Measures should be considered to minimize the negative effects of the use of cryptography on the investigation of criminal offenses, without affecting its legitimate use more than is strictly necessary.

In 1997, the Council of Europe formed a Committee of Experts on Crime in Cyber-space (PC-CY). The group met in secret for several years drafting an international treaty and in April 2000, released the "Draft

Convention on Cyber-crime, version 19." A number of subsequent versions were released until version 27 was released in June 2001.

The convention has three parts. Part I proposes the criminalization of online activities such as data and system interference, the circumvention of copyright, the distribution of child pornography, and computer fraud. Part II requires ratifying states to pass laws to increase their domestic surveillance capabilities to cater for new technologies. This includes the power to intercept Internet communications, gain access to traffic data in real-time or through preservation orders to ISPs, and access to secured or "protected" data. The final part of the treaty requires all states to cooperate in criminal investigations. So, for example, country A can request country B to utilize any of the aforementioned investigative powers within country B for a crime that is being investigated in country A. There is no requirement for the crime in country A to actually qualify as a crime in country B, i.e. no requirement for dual-criminality. In this sense, the convention is the largest mutual legal assistance regime in criminal matters ever created.

The draft convention text was strongly criticized by a wide variety of interested parties including privacy and civil liberties groups for its promotion of surveillance and lack of controls such as authorization requirements and dual criminality;[38] prominent security experts for previously articulated limitations on security software;[39] and industry for the costs of implementing the requirements, and the challenges involved in responding to requests from 43 different countries. The European Union's Data Protection Working Group has expressed concern regarding the convention's implications upon privacy and human rights, concluding that:

> The Working Party therefore sees a need for clarification of the text of the articles of the draft convention because their wording is often too vague and confusing and may not qualify as a sufficient basis for relevant laws and mandatory measures that are intended to lawfully limit fundamental rights and freedoms.[40]

The convention text was finalized in September 2001. After the terrorist attacks on the United States, the convention was positioned as a means of combating terrorism. A signing ceremony took place in November where it was signed by thirty countries, and later signed by another four. Only one country, Albania, has ratified the convention at the time of publication of this report. The Convention is open to the members of the

Council of Europe and to countries that were involved in the development, which includes the United States, Canada, Japan and South Africa. All members of the latter group have signed on.

The convention will come in to force once ratified by five signatories states, of which three must be members of the Council of Europe. Once it is in force, other non-COE countries like China and Singapore can also ask to join. The Australian government announced in July 2001 that its bill on computer crime, which requires users to provide encryption keys, is based on the Convention.[41]

A draft protocol on Racism and Xenophobia is currently under consideration.[42] This protocol apparently will require the criminalization of certain forms of Internet speech that some might find offensive. There was some discussion of a second protocol on "terrorist messages and the decoding thereof," however discussion on this matter has not advanced publicly.[43]

G-8

The Group of 8 (G-8) is made up of the heads of state of eight industrialized countries in the world (Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States. The European Commission participates as an observer). The leaders have been meeting annually since 1975 to discuss issues of importance, including economics and finance, transnational organized crime, terrorism, and the information society.

Since 1995, the G-8 has become increasingly more involved in the issue of high-tech crime, and has created working groups and issued a series of communiqués from the leaders and actions plans from justice ministers. Much of this work has been coordinated by the Lyon Group, established formally in 1997.

At the Birmingham, England summit in May 1998, the G-8 adopted a recommendation on ten principles and a ten-point action plan on high-tech crime. The ministers announced:

> We call for close cooperation with industry to reach agreement on a legal framework for obtaining, presenting and preserving electronic

> data as evidence, while maintaining appropriate privacy protection, and agreements on sharing evidence of those crimes with international partners. This will help us combat a wide range of crime, including abuse of the Internet and other new technologies.

The G-8 has met several times with industry and is actively promoting requirements that Internet Service Providers maintain records of all of their users' activities in case there is a future need to investigate a crime that might have occurred. These requirements were strongly criticized at a meeting held by the G-8 in Japan in 2001 where industry and a civil liberties group were invited. A draft press release and guidelines that promoted data retention had to be withdrawn after they had already been made public.

The G-8 has continued its activity in the area of law enforcement and combating terrorism, however. Throughout 2002 a number of summits involving Finance Ministers, Justice and Interior Ministers, and heads of state have released a number of statements regarding increased surveillance, traceability of communications,[44] and data retention.[45] Increased cooperation across borders was discussed at length; and as with the Council of Europe convention, no requirements of dual-criminality or double-criminality are necessary.

The European Union

In July 2000, the Commission announced plans for a new directive for fighting cyber-crime.[46] A communication was released in January 2001.[47] While similar to the Council of Europe convention in many ways, the Commission's proposal also included proposals regarding data retention and the reduction of anonymity. These policies were sought within "public forums" (only with limited invited speaking slots) in the fall of 2001, with unclear and unpublished results.

The retention proposal was sought in the alternative forum of the electronic services data protection directive in the European Parliament. The substantive law measures of criminalizing data and systems interference and defining other such offences are being pursued as a Council Framework Decision, currently in draft mode.[48] This initiative is designed to be consistent with the Council of Europe and G-8 activities.

Republic of the Philippines

Article III of the Constitution of the Philippines contains the Bill of Rights. Section 1 of the Bill of Rights states that the "Congress shall give highest priority to the enactment of measures that protect and enhance the right of all the people to human dignity".[49] Section 2 states that "the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized".[50] Section 3(1) states that the "privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise, as prescribed by law."[51] It further states that "any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding". Section 7 states that "the right of the people to information on matters of public concern shall be recognized. Access to official records, and to documents and papers pertaining to official acts, transactions, or decisions, as well as to government research data used as basis for policy development, shall be afforded the citizen, subject to such limitations as may be provided by law."[52]

The Supreme Court ruled in July 1998 that Administrative Order No. 308, the Adoption of a National Computerized Identification Reference System, introduced by former President Ramos in 1996, was unconstitutional. The Court found the order, would "put our people's right to privacy in clear and present danger... No one will refuse to get this ID for no one can avoid dealing with government. It is thus clear as daylight that without the ID, a citizen will have difficulty exercising his rights and enjoying his privileges." While stating that all laws invasive of privacy would be subject to "strict scrutiny," the Court also was careful to note that "the right to privacy does not bar all incursions to privacy".[53] President Joseph Estrada reiterated his support for the use of a national identification system in August 1998 stating that only criminals are against a national ID.[54] Justice Secretary Serafin Cuevas authorized the National Statistics Office (NSO) to proceed to use the population reference number (PRN) for the Civil Registry System-Information Technology Project (CRS-ITP) on August 14, claiming that it is not covered by the decision.[55]

There is no general data protection law but there is a recognized right of privacy in civil law.[56] The Civil Code of the Philippines states that "[e]very person shall respect the dignity, personality, privacy, and peace of mind of his neighbors and other persons," and punishes acts that violate privacy by private citizens, public officers, or employees of private companies.[57]

Article 26 of the Civil Code states that "every person shall respect the dignity, personality, privacy and peace of mind of his neighbors and other persons. The following and similar acts, though they may not constitute a criminal offense, shall produce a cause of action for damages, prevention and other relief:

(1) Prying into the privacy of another's residence;

(2) Meddling with or disturbing the private life or family relations of another;

(3) Intriguing to cause another to be alienated from his friends;

(4) Vexing or humiliating another on account of his religious beliefs, lowly station in life, place of birth, physical defect, or other personal condition.[58]

Article 32(11) of the Civil Code states that "any public officer or employee, or any private individual, who directly or indirectly obstructs, defeats, violates or in any manner impedes or impairs the privacy of communication and correspondence shall be liable to the latter for damages."[59]

The Philippines has only one law on data transfer, Presidential Decree (P.D.) No. 1718 entitled "Providing For Incentives In The Pursuit of Economic Development Programs By Restricting The Use of Documents and Information Vital To The National Interest in Certain Proceedings and Processes." While the law was passed in 1980, it lacks force because rules and regulations have not been issued to allow enforcement. Broadly, P.D. 1718 prohibits the export of all documents and information from the Philippines to other countries that may adversely affect the interests of Philippine corporations, individuals, or government agencies. P.D. 1718 contains exceptions for exportation of information that are a matter of form, in connection with business transactions or negotiations that require

them, in compliance with international agreements, or made pursuant to authority granted by the designated representative of the President.[60]

Bank records are protected by the Bank Secrecy Act[61] and the Secrecy of Bank Deposits Act,[62] the latter provides that all deposits of whatever nature with banks or banking institutions are absolutely confidential and may not be examined, inquired, or looked into by any person, government official, bureau or office, absent exceptional circumstances. Those circumstances include: the written permission of the depositor, cases of impeachment, court orders in cases of bribery or dereliction of duty of public officials, cases where the money deposited or invested is the subject matter of litigation, and cases covered by the Anti-Graft and Corrupt Practices Act.[63] Ernest Leung, the president of the Philippine Deposit Insurance Corporation, has made several attempts to eliminate the deposit secrecy act because he believes that no less than total access can ensure the stability of the Philippines banking system.[64] In March 2001, the Senate debated a proposal to force three million citizens to file an annual "Statement of Assets and Liabilities."[65]

In May 2000, the ILOVEYOU e-mail virus was traced to a hacker in the Philippines, focusing international attention on the country's cyberlaw regime. The lack of any internet-specific laws frustrated investigation efforts, and prosecutors finally were able to gain a warrant under the Access Devices Regulation Act of 1998,[66] a law intended to punish credit card fraud that outlaws the use of unauthorized access devices to obtain goods or services broadly.[67]

In May 2000, on the heels of the virus attack, President Joseph Estrada signed into law the Electronic Commerce Act of 2000.[68] Section 3(e) of the Electronic Commerce Act of 2000[69] stipulates the "protection of users, in particular with regard to privacy, confidentiality, anonymity and content control" through policies "driven by choice, individual empowerment, and industry-led solutions". Further, wherever possible, "business should make available to consumers and, where appropriate, business users the means to exercise choice with respect to privacy, confidentiality, content control and, under appropriate circumstances, anonymity".[70] Section 23 mandates a minimum fine of P100,000 (~$2000) and a prison term of six months to three years for unlawful and unauthorized access to computer systems. Section 31 provides that only individuals with legal right of possession shall be granted access to electronic files or electronic keys.

Section 32 imposes an obligation of confidentiality on persons receiving electronic data, keys, messages, or other information not to convey it to any other person.[71]

In June of 2001 the Philippine National Bureau of Investigation (NBI) announced their intention to bring the first formal hacking and piracy charges under the Electronic Commerce Act. The charges involve two former employees of a business school who allegedly broke into the school's computer system and stole an undisclosed amount of proprietary digital material.[72]

While restrictions on search and seizure within private homes are generally respected, searches without warrants do occur. In August of 2000, the Philippine National Police (PNP) conducted random searches of person for illegal firearms at checkpoints in Manila that their own government characterized as in violation of citizen's privacy rights.[73]

The Act to Prohibit and Penalize Wire Tapping and Other Related Violations of the Privacy of Communication and for Other Purposes[74] contains a notwithstanding clause that supersedes all inconsistent statutes.[75] Section 1 states that all parties to a communication must give permission for a recorded wiretap or intercept and makes it illegal to knowingly possess any recording made in prohibition of this law, unless it is evidence for a trial, civil or criminal.[76] Section 2 assesses liability for any person who contributes to the actions described in Section 1.[77] Section 3 provides certain exceptions to the conditions found in sections 1 to 2 but adopts stringent criteria for wiretap warrants, including the identity of the wiretap target; who may execute the warrant; reasonable grounds that a crime has been, is or will be committed; and, a reasonable belief that the evidence obtained via the wiretap will aid in a conviction or prevention of a crime.[78] Further, predicate offenses - or offences for which a court may authorize a wiretap - are limited to a number of particularly onerous severity.[79] Section four states that any communication obtained in violation of this Act shall not be admissible as evidence in any court.

In April 1999, the NBI and the Ombudsman started investigations after reports that police had tapped up to 3,000 telephone lines including top government officials, politicians, religious leaders, businessmen and print and television journalists. In May 1998, Director Gen. Santiago Alino, PNP chief, ordered an investigation of the alleged electioneering and illegal

wiretapping activities by members of the National Police's Special Project Alpha (SPA). The House and the Senate held investigations in August 1997 after officials of the telephone company admitted that their employees were being paid to conduct illegal wiretaps.[80]

Section 5 of the Rape Victim Assistance and Protection Act of 1998, stipulates that "any stage of the investigation, prosecution and trial of a complaint for rape, the police officer, the prosecutor, the court and its officers, as well as the parties to the complaint shall recognize the right to privacy of the offended party and the accused." It further states that a police officer, prosecutor or court may order a closed-door investigation, prosecution or trial and that the name and personal circumstances of the offended party and/or the accused, or any other information tending to establish their identities, and such circumstances or information on the complaint shall not be disclosed to the public.[81] Section 3 provides for the establishment of a rape crisis center in every province and city "for the purpose of: ensuring the privacy and safety of rape victims."[82]

Section 8 of the Proposed Rule on Juveniles in Conflict with the Law stipulates that "the right of the juvenile to privacy shall be protected at all times. All measures necessary to promote this right shall be taken, including the exclusion of the media."[83] Section 9 of the Rule, dealing with the fingerprinting and photographing of a juvenile, states "while under investigation, no juvenile in conflict with law shall be fingerprinted or photographed in a humiliating and degrading manner" and stipulates procedural guidelines such as separate storage of fingerprint files from adult files; restricted access by prior authority of the Family Court; and automatic destruction if no charges are laid or when the juvenile reaches the age of majority (21). Section 26(k) of the Rule confers a duty on the Family Court to respect the privacy of minors during all stages of the proceedings.[84]

The Local Government Code of the Philippines[85] provides all barangay[86] "proceedings for settlement shall be public and informal provided that the... chairman... may upon request of a party, exclude the public from the proceedings in the interest of privacy, decency, or public morals."[87]

Section 14 of Alien Social Integration Act of 1995[88] provides that "information submitted by an alien applicant pursuant to this Act, shall be used only for the purpose of determining the veracity of the factual

statements by the applicant or for enforcing the penalties prescribed by this Act."[89]

The use of biometric technologies has been rising in the Philippines. Since March of 1996, dozens of companies and government agencies have adopted fingerscan technologies in applications ranging from time management and payroll systems to security access control. Many companies use the technology primarily to reduce fraudulent time card punching.[90] Banks use the technology to reduce fraudulent transactions and to promote security. Additionally, GTE and IriScan Inc. introduced iris-scan technology in 1998 to ensure the security of online transactions. Other uses of biometric technology in the Philippines include the dispensation of health care and social services; privacy systems for database and records protection; travel security systems with passport, ticket, and baggage verification; business, residence, and vehicle security with access and operator authentication; processing and circulation control in the corrections or prison environment; and portable systems for on-scene recognition of individuals for use in law enforcement.[91]

In July of 2001 the Philippines' Civil Service Commission released a resolution requiring all government officials and employee to refrain from sending indecent messages. The resolution takes effect on August 5, 2001 and bans public officials from sending sexist jokes, pornographic pictures and lewd letters or mails through electronic means including mobile phones, fax machines and e-mails. Individuals who feel sexually harassed may report cases directly to the Civil Service Commission. The resolution is a follow-up to a proposal by the Commission on Elections and the National Telecommunications Commission to monitor, track and prosecute senders of "politically motivated text messages."[92]

The Code of Conduct and Ethical Standards for Public Officials and Employees[93] mandates the disclosure of public transactions and guarantees access to official information, records or documents. Agencies must act on a request within 15 working days from receipt of the request. Complaints against public officials and employees who fail to act on request can be filed with the Civil Service Commission or the Office of the Ombudsman.

A recent study by MasterCard Inc. entitled "Asian Ideals," indicates that individuals in the Philippines have a moderate level of confidence in the confidentiality of their personal information. The survey included 400

respondents each from 13 different Pacific Rim countries. The privacy portion of the survey used a privacy scale with a score of one indicating "absolutely no privacy" and 10 indicating "total privacy." Fourty-one percent of Filipinos gave scores of eight to 10 regarding the confidentiality of their medical records. Another 24 percent gave a middle score of five.[94] With regard to privacy in office e-mail, telephone, and employee records, 23 percent believe they have "enough privacy" (five on the privacy scale) and nine percent believe they have "total privacy" (10 on the scale). On the specific issue of e-mail privacy, 22 percent of Filipinos believe they have "enough privacy." Filipinos have a little less confidence in the privacy of their office telephone conversations with 23 percent believing they have a high level of privacy (eight to 10 on the scale), 22 percent believing they have enough privacy, and 17 percent believing they have "absolutely no privacy."[95] Bank privacy got significantly better scores. Sixty percent of the respondents gave a score of six or higher when asked to rate the privacy of personal information kept at the bank. Twenty-two percent gave a middle score of five, and 19 percent had some apprehension concerning the privacy of their bank accounts. Filipinos consumers also had mixed feelings about privacy and security on the Internet. Twenty-seven percent gave a middle score of five and almost an equal number of respondents believe the Internet is safe and unsafe - 37 percent give a score of four or lower while 36 percent give a score of six or higher. Fifteen percent said that the Internet was "absolutely unsafe" and only one percent said that it is "totally safe."[96]

Endnotes

1 United Nations Resolution 1368 (2001), adopted by the Security Council at its 4370th meeting, September 12, 2001.

2 Council of Europe Committee of Ministers, Declaration of the Committee of Ministers on the fight against international terrorism, adopted by the Committee of Ministers at the 763rd meeting of the Ministers' Deputies, September 12, 2001.

3 Council of Europe Parliamentary Assembly, Recommendation 1534 (2001), Democracies Facing Terrorism, September 26, 2001 (28th Sitting), available at <http://assembly.coe.int/>.

4 Commission of the European Communities, Brussels, Report From The Commission, Overview of European Union action in response to the events of the 11 September and assessment of their likely economic impact, 17.10.2001, COM(2001) 611 final.

5 Statement of G-7 Finance Ministers and Central Bank Governors, Action Plan to Combat the Financing of Terrorism, October 6, 2001.

6 See generally, <http://www1.oecd.org/fatf/>.

7 Criminal Code of Canada, (CC 186(1b)), 2000.

8 Electronic Frontiers Australia, Media Release: Senate Rejects Email Snooping Law - Victory For Online Privacy, June 28, 2002.

9 Statement of Senator Ellison, Minister of Justice and Customs, Senate Official Hansard No.6 2002, June 27, 2002, available at <http://www.aph.gov.au/hansard/senate/dailys/ds270602.pdf>.

10 Roger Gaspar (NCIS), "Looking to the Future : Clarity on Communications Data Retention Law," August 21, 2000, ACPO, ACPO(S), HM Customs & Excise, Security Service, Secret Intelligence Service, and GCHQ,.

11 Letter from President George W. Bush to Mr Romano Prodi, President, Commission of the European Communities, Brussels, October 16, 2001, forwarded by the Deputy Chief of Mission, United States Mission to the European Union, available at < http://www.statewatchchaterorg/news/2001/nov/06Ausalet.htm >

12 Comments of the United States Government on the European Commission Communication on Combating Computer Crime, December 2001, available at <http://www.cybercrime.gov/intl/USComments_CyberCom_final.pdf>.

13 Prepared statement of the United States of America, presented at European Union Forum on Cybercrime, Brussels, 27 November 2001, available at <http://www.cybercrime.gov/intl/MMR_Nov01_Forum.doc>.

14 Statement of the G8 Justice and Interior Ministers: Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations, May 14 2002, Mont Tremblant, Quebec, available at <http://www.g8j-i.ca/english/doc2.html>.

15 The Performance and Innovation Unit of the Cabinet Office, "Privacy and data-sharing: The way forward for public services," April 2002, available at <http://www.cabinet-office.gov.uk/innovation/2002/privacy/report/>.

16 "FIPR appalled by Huge Increase in Government Snooping," Foundation for Information Policy Research Press Release, June 10, 2002, available at <http://www.fipr.org/press/020610snooping.html>.

17 "Chaos warning over airport security plan", BBC News Online, July 6, 2002, availableat <http://news.bbc.co.uk/hi/english/uk/newsid_2104000/2104280.stm>.

18 Solicitor General of Canada, RCMP and CSIS Access to Airline Passenger Information, available at <http://www.sgc.gc.ca/EPub/Pol/eAirPassInfo.htm>.

19 Letter to Honourable David Collenette, Minister of Transport, on the subject of Bill C-55, from the Privacy Commissioner of Canada, George Radwanski, June 18, 2002, available at <http://www.privcom.gc.ca/media/nr-c/02_05_b_020618_e.asp>.

20 "Europol to be given access to the S.I.S., then custody?" Statewatch, March 27, 2002.

21 Glenn R. Simpson and Jathon Sapsford, "New Rules for Money-Laundering," The Wall Street Journal, April 23, 2002.

22 "Financial Action Task Force on Money Laundering Special Recommendations on Terrorist Financing," available at <http://www.fatf-gafi.org/SRecsTF_en.htm>.

23 Robert O'Harrow Jr., "Financial Database To Screen Accounts: Joint Effort Targets Suspicious Activities," Washington Post, May 30, 2002; at E01.

24 "Special Report: New Threats To Privacy: The Intensifying Scrutiny at Airports," Business Week, June 5, 2002.

25 Robert O'Harrow Jr., "Intricate Screening Of Fliers In Works -- Database Raises Privacy Concerns," Washington Post, February 1, 2002, at A01. 26 "Iris Scans Take off at Airports," ComputerWorld, July 17, 2002.

27 Ricardo Alonso-Zaldivar, "Trusted' Air Travelers Would Minimize Wait Security: Passengers who Voluntarily Agree to a Background Check Could be Issued a Special Credential," Los Angeles Times, February 5, 2002.

28 Council of Europe Convention on Cybercrime (ETS no: 185), opened for signature on November 8, 2001.

29 Testimony of the Attorney General to the Senate Committee on the Judiciary, Washington DC, September 25, 2001.

30 See EPIC's Data Retention Page <http://www.epic.org/privacy/intl/data_retention.html>.

31 Directive 2002/_/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (still unpublished). An unofficial consolidated version is available at <http://www.gilc.org/as_voted_2nd_read.html>.

32 Article 15(1), ibid.

33 Article 2(b) and (c), ibid.

34 Open Letter to Mr. Pat Cox, President, European Parliament, from the Global Internet Liberty Campaign, May 2002, at <http://gilc.org/cox_en.html>.

35 This is the case in Spain where the recent law allowing data retention for a year has been challenged as being in direct opposition to the Spanish Constitution. For more details see <http://www.kriptopolis.com/net/tc.php>.

36 Dr Paul Norman, "Policing 'high tech crime' in the global context: the role of transnational policy networks," available at <http://www.bileta.ac.uk/99papers/norman.htm>.

37 For details see <http://www.privacyinternational.org/issues/cybercrime/>.

38 See, for example, Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime, October 18, 2000 at <http://www.gilc.org/privacy/coe-letter-1000.html>; and Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime Version 24.2, December 12, 2000 at <http://www.gilc.org/privacy/coe-letter-1200.html>.

39 Statement of Concerns, July 20, 2000. <http://www.cerias.purdue.edu/homes/spaf/coe/index.html>.

40 European Union Article 29 Data Protection Working Group, Opinion 4/2001On the Council of Europe's Draft Convention on Cyber-crime, March 22, 2001

41 Cybercrime Bill 2001 Second Reading Speech by the Attorney General, The Parliament of the Commonwealth of Australia.

42 See, e.g., Global Internet Liberty Campaign, Member Letter to Council of Europe Secretary-General Walter Schwimmer, February 6, 2002. <http://www.gilc.org/speech/coe_hatespeech_letter.html>.

43 See, e.g., Global Internet Liberty Campaign, Member Letter to Council of Europe Secretary-General Walter Schwimmer, February 28, 2002, <http://www.gilc.org/speech/coe_hatespeech_2.html>.

44 Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations, published at the G8 Justice and Interior Ministers' Meeting in Mont-Tremblant, Quebec, May 2002.

45 Principles on the Availability of Data Essential to Protecting Public Safety, published at the G8 Justice and Interior Ministers' Meeting in Mont-Tremblant, Quebec, May 2002.

46 "European Union Ministers Vow Cyber Crime Crackdown," Reuters, July 29, 2000.

47 Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, Creating a Safer Information Society by Improving the Security of Information Infrastructures

and Combating Computer-related Crime, COM(2000) 890 final, January 26, 2001, available at <http://www.privacyinternational.org/issues/cybercrime/eu/>.

48 Commission Proposal for a Council Framework Decision on Attacks against Information Systems (COM (2002) 173 final), April 19, 2002.; OECD Guidelines for the Security of Information Systems, adopted November 1992, available at <http://www.oecd.org/EN/document/0,,EN-document-29-nodirectorate-no-24-10249-

49 Constitution of the Philippines, article. VIII, § 1.

50 Ibid., p. 2.

51 Ibid., p. 3(1).

52 Ibid., p. 7.

53 Philippine Supreme Court Decision of the National ID System, July 23, 1998, G.R.127685, available at <http://bknet.org/laws/nationalid.html>.

54 'Erap wants nat'l ID system (Only criminals disagree with it, says the President),' Business World (Manila), August 12, 1998.

55 Opinion Number 91; See "Foundation laid for proposed Nat'l ID," Business World (Manila), August 14, 1998.

56 Cordero v. Buigasco, 34130-R, April 17, 1972, 17 CAR (2s) 539; Jaworski v. Jadwani, CV-66405, December 15, 1983.

57 Civil Code, article 26; See n. 35 of the Philippine Supreme Court Decision of the National ID System, supra n.1471.

58 Civil Code, article 26.

59 Ibid., article 32(11).

60 E-com Legal Guide, The Philippines, Christopher Lim, Baker & McKenzie, Manila, January 2001.

61 Bank Secrecy Act, No. 7653.

62 Secrecy of Bank Deposits Act, No. 1405.

63 Internet Banking - Key Legal Considerations, Natividad Kwan and Cornelio B. Abuda, Baker & McKenzie, Manila, November 2000.

64 'Bangko Sentral favor deposit secrecy lifting,' Business World (Manila), (January 17, 2000).

65 House Bill 5345.

66 Access Devices Regulation Act of 1998, No. 8484.

67 Ibid.

68 Electronic Commerce Act of 2000, No 8972.

69 Electronic Commerce Act of 2000, No. 8792.

70 Ibid., Art. 3(e).

71 Internet Banking - Key Legal Considerations, Natividad Kwan and Cornelio B. Abuda, Baker & McKenzie, Manila, November 2000.

72 "Philippines' NBI Clamps Down on 'Cyberthieves,'" Metropolitan Computer Times, June 13, 2001.

73 United States Department of State, Country Report on Human Rights Practices for 2001, March 2002, available at <http://www.state.gov/g/drl/hrrpt/2001/>.

74 Act to Prohibit and Penalize Wire Tapping and Other Related Violations of the Privacy of Communication and for Other Purposes, No. 4200, June 19, 1965.

75 Ibid., p. 5.

76 Ibid., p. 1.

77 Penalties include imprisonment, disqualification from public office or deportation, in the case of a foreign alien.

78 No. 4200, p. 3.

79 Offences falling into this category include: crimes of treason, espionage, provoking war and disloyalty in case of war, piracy, mutiny in the high seas, rebellion, conspiracy and proposal to commit rebellion, inciting to rebellion, sedition, conspiracy to commit sedition, inciting to sedition, kidnapping as defined by the Revised Penal Code, and violations of Commonwealth Act No. 616, punishing espionage and other offenses against national security.

80 "Wiretapping probe," Business World (Manila), August 26, 1997.

81 Rape Victim Assistance and Protection Act of 1998, No. 8505, § 5.

82 Ibid., Art. 3(d).

83 Proposed Rule on Juveniles in Conflict With the Law A. M. NO. 02-1-18-SC, April 15, 2002, available at <http://www.chanrobles.com/amno02118sc.htm>, § 8.

84 Ibid., p. 26.

85 Local Government Code of the Philippines.

86 As the basic political unit, the barangay serves as the primary planning and implementing unit of government policies, plans, programs, projects, and activities in the community, and as a forum wherein the collective views of the people may be expressed, crystallized and considered, and where disputes may be amicably settled.

87 Local Government Code of the Philippines, p. 414.

88 Alien Social Integration Act of 1995, No. 7919.

89 Ibid., p. 14.

90 The Government Service Insurance System, National Computer Center, Philippine Tourism Authority, Department of Social Welfare and Development, and the Light Railway Transit Authority use the figerscan as a means to ensure that employees are actually at the worksite.

91 "Biometrics system usage rises," Business World (Manila), February 17, 1998.

92 "Philippine Agency Acts on 'E-Harrassment' In Gov't Workplaces," Metropolitan Computer Times, July 23, 2001.

93 Republic Act 6713 of 1987.

94 "Spouses are Asians' most trusted family members," Business World (Manila), May 17, 2001.

95 "Asia-Pacific consumers note work privacy," Business World (Manila), March 23, 2001.

96 "Filipinos fairly confident of bank account privacy Mastercard Asain Ideals TM survey shows," Business World (Manila), May 31, 2001.

References

Alonso-Zaldivar, Ricardo "Trusted' Air Travelers Would Minimize Wait Security: Passengers who Voluntarily Agree to a Background Check Could be Issued a Special Credential." Los Angeles Times 05 February 2002.

"Asia-Pacific consumers note work privacy." Business World 23 March 2001.

Australia. Parliament. Cybercrime Bill 2001 Second Reading Speech by the Attorney General.

"Bangko Sentral favor deposit secrecy lifting." Business World 17 January 2000.

"Biometrics system usage rises." Business World 17 February 1998.

Bush, George W. 'To Romano Prodi." 16 October 2001. At http://www.statewatchapterorg/news/2001/nov/06Ausalet.htm.

Canada. Criminal Code, 2000.

"Chaos' warning over airport security plan." BBC News Online. 6 July 2002. At http://news.bbc.co.uk/hi/english/uk/newsid_2104000/2104280.stm.

'Comments of the United States Government on the European Commission Communication on Combating Computer Crime.' December 2001. At http://www.cybercrime.gov/intl/USComments_CyberCom_final.pdf.

Commission of the European Communities. Proposal for a Council Framework Decision on Attacks against Information Systems (COM (2002) 173 final). 19 April 2002.

_____. Report From The Commission: Overview of European Union Action in Response to the Events of the 11 September and Assessment of their likely Economic Impact. Brusells: Commission of the European Communities, 2001.

Cordero v. Buigasco. 34130-R, 17 CAR (2s) 539. 17 April 1972.

Council of Europe Committee of Ministers. Declaration of the Committee of Ministers on the Fight against International Terrorism. Adopted by the Committee of Ministers at the 763rd meeting of the Ministers' Deputies, September 12, 2001.

Council of Europe Parliamentary Assembly. Recommendation 1534: Democracies Facing Terrorism. 26 September 2001 (28th Sitting) At http://assembly.coe.int/.

'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890 final." 26 January 2001. At http://www.privacyinternational.org/issues/cybercrime/eu/.

Electronic Frontiers Australia. "Senate Rejects Email Snooping Law - Victory For Online Privacy." 28 June 2002.

EPIC. "Data Retention." At http://www.epic.org/privacy/intl/data_retention.html.

'Erap wants nat'l ID system (Only criminals disagree with it, says the President)." Business World 12 August 1998.

European Parliament and the European Council. Directive 2002. At http://www.glc.org/as_voted_2nd_read.html.

European Union. Article 29 Data Protection Working Group, Opinion 4/2001 On the Council of Europe's Draft Convention on Cyber-crime. 22 March 2001.

"European Union Ministers Vow Cyber Crime Crackdown." Reuters 29 July 2000.

"Europol to be given access to the S.I.S., then custody?" Statewatch 27 March 2002.

"Filipinos fairly confident of bank account privacy Mastercard Asain Ideals TM survey shows." Business World 31 May 2001.

"Financial Action Task Force on Money Laundering Special Recommendations on Terrorist Financing." At http://www.fatf-gafi.org/SRecsTF_en.htm.

Foundation for Information Policy Research. "FIPR appalled by Huge Increase in Government Snooping." 10 June 2002. At http://www.fipr.org/press/020610snooping.html.

"Foundation laid for proposed Nat'l ID." Business World 14 August 1998.

G-7 Finance Ministers and Central Bank Governors. Action Plan to Combat the Financing of Terrorism, October 6, 2001.

G8 Justice and Interior Ministers. "Principles on the Availability of Data Essential to Protecting Public Safety." Mont-Tremblant, Quebec: G8 Justice and Interior Ministers, May 2002.

_____. "Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations." 14 May 2002. At http://www.g8j-i.ca/english/doc2.html.

_____. "Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations." Mont-Tremblant, Quebec: G8 Justice and Interior Ministers, May 2002.

Gaspar, Roger "Looking to the Future : Clarity on Communications Data Retention Law," ACPO, ACPO(S), HM Customs & Excise, Security Service, Secret Intelligence Service, and GCHQ, 2000.

Global Internet Liberty Campaign. "To Council of Europe Convention on Cyber-Crime." 18 October 2000. At http://www.gilc.org/privacy/coe-letter-1000.html.

_____. "To Council of Europe Convention on Cyber-Crime." 12 December 2000. At http://www.gilc.org/privacy/coe-letter-1200.html.

_____. "To Council of Europe Secretary-General Walter Schwimmer." 06 February 2002. At http://www.gilc.org/speech/coe_hatespeech_letter.html.

_____. "To Council of Europe Secretary-General Walter Schwimmer." 28 February 2002. At http://www.gilc.org/speech/coe_hatespeech_2.html.

_____. "To Pat Cox." May 2002. At http://gilc.org/cox_en.html.

'Iris Scans Take off at Airports." ComputerWorld 17 July 2002.

Jaworski v. Jadwani. CV-66405. 15 December 1983.

Kwan, Natividad and Abuda, Cornelio B. Internet Banking - Key Legal Considerations.Manila: Baker & McKenzie, 2000.

Lim, Christopher. E-com Legal Guide: The Philippines.Manila: Baker & McKenzie, 2001.

'New Threats To Privacy: The Intensifying Scrutiny at Airports." Business Week 05 June 2002.

Norman, Paul. "Policing 'high tech crime' in the global context: the role of transnational policy networks." At http://www.bileta.ac.uk/99papers/norman.htm.

O'Harrow, Robert Jr. "Financial Database To Screen Accounts: Joint Effort Targets Suspicious Activities." Washington Post 30 May 2002: E01.

O'Harrow, Robert Jr. 'Intricate Screening Of Fliers In Works -- Database Raises Privacy Concerns.' Washington Post 01 February 2002: A01.

Organization for Economic Cooperation and Development. At http://www1.oecd.org/fatf/

_____. Guidelines for the Security of Information Systems. November 1992, At http://www.oecd.org/EN/document/0,,EN-document-29-nodirectorate-no-24-10249-.

'Philippine Agency Acts on 'E-Harrassment' In Gov't Workplaces." Metropolitan Computer Times 23 July 2001.

'Philippines' NBI Clamps Down on 'Cyberthieves," Metropolitan Computer Times 13 June 2001.

Philippines. 1987 Constitution.
Philippines. Civil Code.
Philippines. Commonwealth Act No. 616.
Philippines. Congress. House Bill 5345.
Philippines. Local Government.
Philippines. Republic Act No. 1405.
Philippines. Republic Act No. 4200.
Philippines. Republic Act No. 6713.
Philippines. Republic Act No. 7653.
Philippines. Republic Act No. 7919.
Philippines. Republic Act No. 8484.
Philippines. Republic Act No. 8505.
Philippines. Republic Act No. 8972.

Philippines. Revised Penal Code.

"Prepared statement of the United States of America, presented at European Union Forum on Cybercrime." 27 November 2001. At http://www.cybercrime.gov/intl/MMR_Nov01_Forum.doc.

Radwanski, George. "To David Collenette." 18 June 2002. At http://www.privcom.gc.ca/media/nr-c/02_05_b_020618_e.asp.

Simpson, Glenn R. and Sapsford, Jathon "New Rules for Money-Laundering." The Wall Street Journal 23 April 2002.

"Solicitor General of Canada, RCMP and CSIS Access to Airline Passenger Information." At http://www.sgc.gc.ca/EPub/Pol/eAirPassInfo.htm.

"Spouses are Asians' most trusted family members," Business World 17 May 2001.

"Statement of Concerns." 20 July 2000. At http://www.cerias.purdue.edu/homes/spaf/coe/index.html.

"Statement of Senator Ellison, Minister of Justice and Customs, Senate Official Hansard No.6 2002." 27 June 2002. At http://www.aph.gov.au/hansard/senate/dailys/ds270602.pdf.

"Supreme Court Decision of the National ID System." 23 July1998. At http://bknet.org/laws/nationalid.html.

United Kingdom.The Performance and Innovation Unit of the Cabinet Office. "Privacy and data-sharing: The way forward for public services." April 2002. At http://www.cabinet-office.gov.uk/innovation/2002/privacy/report/.

United Nations. Resolution 1368. Adopted by the Security Council at its 4370th Meeting, September 12, 2001.

United States. Department of State. "Country Report on Human Rights Practices for 2001." March 2002. At http://www.state.gov/g/drl/hrrpt/2001/.

_____. Senate. Testimony of the Attorney General to the Senate Committee on the Judiciary. Washington DC, September 25, 2001.

"Wiretapping probe." Business World 26 August 1997.