Appendix: Security and Privacy Institutional Arrangements: Australia and India

Australia

Introduction

The Commonwealth of Australia is a federation of states. The purposes for which the Commonwealth was established are known and (to an extent) codified within the Australian Constitution. There are a number of sections in the *Constitution of the Commonwealth of Australia* that explicitly establish a framework for law enforcement activities. These are:

Section 51:

(xxiv) The service and execution throughout the Commonwealth of civil and criminal process and the judgments of the courts of the States:

And:

Section 119: The Commonwealth shall protect every State against invasion and, on the application of the Executive Government of the State, against domestic violence.

Having said this, the Constitution is silent concerning which rights (if any) of citizens are meant to be served by the government. To that extent, there is a problem in discerning the limiting factors that ought to serve as the boundaries within which the Commonwealth pursues its law enforcement activities. In fact, the absence of a Bill of Rights (or some equivalent document) leaves this important question unresolved except in the following circumstances:

1. Where the Commonwealth legislates to create a right.
2. Where a treaty to which the Commonwealth is a party creates a right (as in the United Nations Declaration of Human Rights).
3. Where the courts discern that a right exists under the common law.
4. Where the courts find that a stated or implied right exists under the Constitution.

Although the Commonwealth has law enforcement powers and agencies, law enforcement is and remains primarily a state responsibility, and each of the states has its own police service (e.g. New South Wales Police, Victoria Police).

Moreover, although there is no Commonwealth Bill of Rights, one of the states (Victoria) and one of the territories (Australian Capital Territory (ACT)) have recently introduced human rights legislation (Victoria's Charter of Human Rights and Responsibilities Act 2006 and the ACT Human Rights Act 2004), and each requires that any statutory provisions that are found to be incompatible with the human rights thus established are identified and a justification provided. However, the relevant parliaments are not required to rescind legislation that is found to be incompatible with the relevant human rights legislation. Both the Victorian and ACT human rights legislation explicitly establish a human right to privacy. There are also moves afoot to establish a Commonwealth Bill of Rights (Brennan Commission of Inquiry).

Some of the key federal agencies relevant to security and privacy are those with law enforcement or defense functions and their respective oversight bodies.

Regarding law enforcement, key agencies include the Australian Federal Police (AFP), the Australian Crime Commission (ACC) and Australian Transaction Reports and Analysis Centre (AUSTRAC). The AFP has an analogous role to that of the FBI. For example, it is concerned with serious trans-jurisdictional crimes, such as organized crime and terrorism. The focus of the ACC is on organized crime; its functions include collecting and analyzing criminal intelligence and maintaining criminal intelligence systems. AUSTRAC gathers and analyzes information about financial transactions. The various Australian police databases of information, including those containing names and details of offenders (photographs, fingerprints, criminal history, outstanding warrants and, in many cases, DNA records), names of gun owners and missing persons, listed telephone numbers and addresses, stolen cars and names and aliases of ''persons of interest'' are linked through the National Police Reference System. An important oversight body is the Australian Commission for Law Enforcement Integrity (ACLEI). The main focus of ACLEI is the prevention, detection and investigation of serious corruption in federal law enforcement agencies. The Parliamentary Joint Committee on the Australian Crime Commission is the main oversight body for that organization.

Regarding intelligence and defense intelligence, key agencies include (in regard to intelligence) the Australia Security Intelligence Organization (ASIO), the Australian Secret Intelligence Service (ASIS) and (in regard to defense intelligence) the Defence Intelligence Organisation (DIO). ASIO is principally concerned with the domestic security of Australia; it has both an intelligence collection role and an assessment role. Security in this context means the protection of Australia from espionage, sabotage, attacks on the Australian defense system, terrorism

and the like. ASIS collects intelligence outside Australia and engages in counter-intelligence. DIO assesses foreign intelligence and exists principally to support the Department of Defence. An important oversight body is the Inspector-General of Intelligence and Security (IGIS). The latter is an independent statutory officer responsible for ensuring that the activities of the intelligence and defense agencies are lawful and have appropriate regard to human rights, including privacy.

The Office of the Privacy Commissioner is the federal agency with responsibility for overseeing the operation of the key piece of Australian legislation pertaining to privacy, namely, the Privacy Act 1988. Most law enforcement agencies in Australia are covered by the Privacy Act, including the AFP and AUSTRAC, though the ACC is exempt. The intelligence and defense intelligence agencies are partially or completely exempt from the Privacy Act.

Some of the key pieces of federal legislation pertaining to security and privacy are: the Privacy Act 1988 (in partial fulfillment of Australia's international obligations under the International Covenant on Civil and Political Rights, which recognizes a basic right to privacy); the Anti-Money Laundering and Counter-terrorism Financing Act 2006; the Telecommunications (Interception and Access) Act 1979; the Telecommunications Act 1997; the Surveillance Devices Act 2004 (which outlines the circumstances under which surveillance devices can be used by federal law enforcement agencies in particular); the Freedom of Information Act 1982 (which outlines the rights of access of individuals to government-held documents); and the Data-matching Program (Assistance and Tax) Act 1990 (which regulates data-matching that makes use of tax file numbers). In addition, the states have legislation in relation to privacy and various associated agencies, such as privacy commissioners.

In Australia, no jurisdiction has legislated into existence a cause of action for invasion of privacy; rather, any such cause of action is part of the common law.

In Australia, identity theft is not currently a federal offense. However, it is a federal offense to dishonestly obtain or deal in personal financial information without the consent of the relevant person. Although the legislation clearly captures credit card fraud and a range of other kinds of identity fraud/theft, it is not clear that it is wholly adequate.

The Privacy Act 1988 and privacy principles

The Privacy Act gives effect to Article 17 of the International Covenant on Civil and Political Rights and the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The Privacy Act regulates the collection, use, storage, disclosure and correction of personal information. The requirements

of the Act include the National Privacy Principles (NPP) (applying to private sector organizations) and the Information Privacy Principles (IPP) (applying to Australian government agencies).

The NPP include principles that relate to: (1) collection of information by an organization from an individual (e.g. that information collection is lawful, not unreasonably intrusive or necessary for one of the organizations purposes); (2) use and disclosure (e.g. that information is lawful, is consented to by an individual, is necessary to prevent serious or imminent threat to life or is not sensitive); (3) data quality (e.g. that information is accurate and up-to-date); (4) data security (e.g. that information is protected from unauthorized access by members of an organization); (5) openness (e.g. that an organization make available how it manages personal information); (6) access and correction (e.g. that an individual has access to information about him/herself, unless providing access would be unlawful); (7) identifiers (e.g. that an organization not adopt as its own identifier of an individual an identifier of the individual that has been assigned by a government agency – to reduce the possibility of data-matching); (8) anonymity (e.g. that individuals have the option of not identifying themselves in transactions with organizations); (9) transborder data flows (e.g. a presumption against transfer of personal information to someone in a foreign country); and (10) sensitive information (e.g. a presumption against the collection of sensitive information).

The IPP consists of most of the principles constitutive of the NPP. However, it does so in the context of some requirements specific to Commonwealth agencies, for example, with respect to legal requirement for archival record-keeping. Moreover, there are some important differences. For example, unlike the IPP, under the NPP there is no obligation to destroy or de-identify personal information data when they are no longer required for the purpose for which they were originally collected.

Agencies

Office of the Privacy Commissioner (OPC)

The OPC's responsibilities include overseeing and monitoring compliance with the Privacy Act (see below), investigating breaches of the Data-matching Program (Assistance and Tax) Act 1990 and monitoring compliance with record-keeping requirements of the Telecommunications Act 1997. As a consequence, the OPC conducts audits and examines records, receives and investigates privacy complaints and enforces the acts through determinations and court proceedings.[1]

1 See *The Operation of the Privacy Act: Annual Report 2008–2009* (Canberra: Office of the Privacy Commissioner, 2009).

The Australian government has announced the establishment of a new statutory Office of the Information Commissioner, to be headed by an Information Commissioner, but which will also include the Privacy Commissioner and a Freedom of Information Commissioner (another new statutory office).

The Privacy Commissioner is a member of various government committees and groups, such as the National Identity Security Group, convened by the Attorney-General's Department, and in these fora the Privacy Commissioner provides advice on privacy issues.

The OPC is an active participant in various international organizations (e.g. the Organization for Economic Cooperation and Development (OECD)), fora (e.g. Asia Pacific Privacy Authorities Forum) and developments (such as the Asia Pacific Economic Cooperation (APEC) Data Privacy Pathfinder, endorsed by the APEC economies under the APEC Privacy Framework). Under the Pathfinder work plan are projects such as cooperation arrangements for cross-border cooperation on privacy enforcement and cross-border complaint handling.

The OPC makes numerous submissions to government and elsewhere. For example, in 2009 the OPC made a submission to the Australian Law Reform Commission's Review of Secrecy Laws on secrecy laws and, specifically, the interaction between secrecy laws and the Privacy Act.[2] Among other things, the OPC recommended "that where an agency identifies a need to require or authorize the handling of personal information where that handling would otherwise breach the Privacy Act, the agency should have a clear and appropriate policy basis for doing so."[3]

Although the Privacy Act applies to private sector organizations as well as Australian government agencies, the OPC does not have the power to conduct audits of organizations in the private sector. Moreover, there are various public sector agencies that are exempt from the Privacy Act and, therefore, from oversight and monitoring by the OPC (see below). Further, the Privacy Act does not cover businesses with less than AU$3 million annual turnover (i.e. the majority of businesses in Australia).

The federal Privacy Act does not cover state public sector agencies and the OPC does not have jurisdiction with respect to state public sector agencies. These come under the jurisdiction of the various state privacy commissioners (e.g. the Office of the Victorian Privacy Commissioner) and are covered by state legislation. However, not all the states have privacy legislation or privacy commissioners – Western Australia, for example, does not. Moreover, some state law enforcement agencies have partial exemptions from the relevant state

2 Australian Law Reform Commission, *Review of Secrecy Laws* – Issues Paper 34 (2009).
3 *Annual Report 2008–09*,1.4.1.

privacy legislation. Victoria Police, for example, does not have to comply if it has a reasonable belief that, in relation to a particular matter, compliance would prevent it from conducting its law enforcement function.

In Australia, other than the Victorian Commissioner for Law Enforcement Data Security, there is no statutory body concerned exclusively with data security. At the federal level and in other states data security and, specifically, law enforcement data security are simply functions of oversight agencies with a wider remit. Thus the Crime and Conduct Commission in Queensland oversees the Queensland Police (and other Queensland public sector agencies) and has a concern with data security.

Australian Security Intelligence Organisation (ASIO)

As stated above, ASIO is responsible for protecting Australia and Australians from espionage, sabotage, attacks on the Australian defense system, terrorism and the like; moreover, ASIO has both an intelligence collection and an assessment role.

ASIO collects security information under warrant and only the Director-General of Security or an ASIO officer authorized by the Director-General can communicate such information. Under the Attorney-General's guidelines articulated in the Performance by the Australian Security Intelligence Organization of its Function of Obtaining, Correlating, Evaluating and Communicating Intelligence relevant to Security (including Politically Motivated Violence),[4] ASIO must: obtain intelligence in a lawful and timely manner; ensure the means it uses to obtain information are proportionate to the threat; and ensure such means are the least intrusive possible. The Director-General must ensure that any personal information held or disclosed is accurate and protected against unauthorized disclosure.

As noted earlier, ASIO's compliance with the Attorney-General's guidelines is overseen by the Inspector-General of Intelligence and Security (IGIS). The IGIS has access to ASIO's records and the power to require persons to answer questions and produce documents, including documents with a national security classification.

However, ASIO is exempt from the Privacy Act and the Freedom of Information Act. In addition, according to the Australian Law Reform Commission's Privacy Inquiry, the privacy rules that are applicable to ASIO do not cover persons who are not Australian citizens.[5] Nevertheless, these rules need to be updated with respect to classified (as opposed to security-classified) information in respect of the incorrect disclosure, accuracy of records and storage of personal information.

4 Available at: www.asio.gov.au/About/Content/AttorneyAcountability.aspx.

5 Australian Law Reform Commission, *Australian Privacy Law and Practice* – Report 108 (2008), 17–18, available at: http://www.austlii.edu.au/au/other/alrc/publications/reports/108/.

Australian Crime Commission (ACC)

As stated earlier, the focus of the ACC is on organized crime. The ACC's projects have included drug trafficking, targeting suspected pedophile rings and determining the nature and extent of organized crime within particular ethnic communities. The ACC has the full array of intrusive law enforcement powers, such as the use of surveillance devices, the capacity to intercept telephone and internet communications, the use of undercover operatives and participation in controlled operations ("traps"). In addition, the ACC has special powers that are not possessed by normal law enforcement agencies, such as the power to issue a summons requiring a person to give evidence under oath and for which failure to attend may attract imprisonment. The ACC also provides strategic and tactical intelligence to other law enforcement agencies in relation to serious crimes, including murder and violent crime, drug trafficking, fraud, organized motor vehicle theft, organized gambling and extortion.

As mentioned above, the functions of the ACC include collecting and analyzing criminal intelligence and maintaining criminal intelligence systems. The ACC uses and adds to a variety of criminal intelligence data bases. It deploys techniques such as data-matching and profiling. As noted elsewhere in this study, profiling consists of developing a profile or set of characteristics of an offender or class of offenders, based in part on the characteristics of the types of person who commit that sort of crime. Once a profile has been developed, people with that profile can become the subjects of targeted investigations.

Besides data provided by law enforcement agencies, including surveillance sheets, the ACC relies on data from public records, company records, the National Missing Persons Unit, Telstra and government departments, including taxation, social security, health and immigration. Although provision of confidential information by these government departments is at the discretion of these departments, it is usually provided after a request from the ACC. Such requests are made for the general reason that the information will assist investigation into a serious crime.

As noted above, the Privacy Act does not apply to the ACC; nor does the Freedom of Information Act. The ACC does not destroy but archives information that it possesses, including transcripts and files on individuals. Although there are audit trails on ACC activities, it is not known whether there are procedures in place that actually monitor these audit trails.

In the area of organized crime, there is some tension between privacy and law enforcement. This tension is especially evident with respect to third parties – that is, persons who are not themselves suspects but who communicate with suspects whose communications are being intercepted.

Whether the ACC should be exempted from the Privacy Act is an issue that remains unresolved. One option here would be to bring the ACC under the Privacy Act, albeit *qua* law enforcement body (as is the case with, for example, the AFP). This would ensure it was subject to privacy principles, except to the extent that its law enforcement activities exempted it. The view of the Australian Law Reform Commission is that the ACC should remain exempt from the Privacy Act, but that: ''The Australian Crime Commission (ACC) in consultation with the Privacy Commissioner, should develop and publish information-handling guidelines for the ACC and the Board of the ACC.''[6] In that case, the Parliamentary Joint Committee on the Australian Crime Commission should then monitor the ACC's compliance with these guidelines.

Australian Transaction Reports and Analysis Centre (AUSTRAC)

Under the Anti-Money Laundering and Counter-terrorism Financing Act 2006 and related legislation, AUSTRAC concerns itself with money laundering activities. Illegal activities, such as drug dealing and major fraud, generate large amounts of money that need to be laundered. In addition, terrorist organizations seek to acquire and transfer funds illegally. One of the most effective ways of combating these kinds of crime is to follow the so-called money trail. AUSTRAC gathers and analyzes data about financial transactions, and the data – at least in the first instance – is of two kinds: (1) data automatically provided in accordance with the law, including domestic bank and other transactions over $10,000, and international telegraphic transfers over $5,000; and (2) data furnished in suspect transaction reports (STRs) on the basis of the discretionary judgment of bank tellers and the like. These discretionary judgments are based on ''suspicious'' behavior or situations – for example, someone apparently structuring deposits in such a manner as to avoid the $10,000 reporting requirement. (STRs go directly to law enforcement agencies as well as AUSTRAC.)

These two kinds of data are entered on AUSTRAC's database and might provide the starting point for an investigative analysis by AUSTRAC. This investigative analysis might make use of computerized techniques such as data-matching and may have recourse to additional data, the precise nature of which is not publicly available. Should the investigative analysis fail to allay the suspicions that triggered the initial interest of AUSTRAC, the material is handed over to law enforcement agencies for further investigation. For example, frequent deposits in a number of banks by person *X* of sums of $9,900 might trigger an investigative analysis that, because *X* is unemployed, yields no apparently legitimate explanation. Alternatively, *X* might turn out to be a legitimate businessman whose product retails for $9,900.

6 Australian Law Reform Commission, *Australian Privacy Law and Practice*, Recommendation 37–1 (a).

AUSTRAC has some accountability mechanisms covering its activities. For example, its staff will have had their security checked and they have limited access to data. Moreover, their activities leave audit trails, and the Director of AUSTRAC has the right to follow these trails. Nevertheless, although there are audit trails, there is evidently no set of procedures in place that will routinely follow those trails. According to the OPC website's list of agencies audited, the OPC has to date not audited AUSTRAC. Moreover, state agencies that have access to AUSTRAC data may not have the same accountability under the Privacy Act as federal agencies. Specifically, it is unclear whether some state agencies are using AUSTRAC-provided data for purposes other than those provided for in the anti-money laundering and counter-terrorism financing legislation.

In some instances AUSTRAC's capacity to provide data and intelligence in relation to money laundering might be undermined by recent technological developments. For example, money launderers who use smartcard technology, high-level encryption and the internet might be able to make international transfers that bypass the financial system and that are not able to be intercepted.

India

India is a sovereign democratic republic and a British Commonwealth nation; in fact, this former British colony is the world's largest democracy. India has the parliamentary form of a union government and a unitary construction of twenty-eight states – each with its own elected legislative assembly – and seven union territories administered by India's union government.

The Constitution of India provides for various Fundamental Rights (e.g. the protection of life and personal liberty (Article 21)) that cannot be removed by the state and that are legally enforceable against the state. The Constitution is interpreted by the Supreme Court, and states that "the law declared by the Supreme Court shall be binding within the terrority of India" (Article 141).

India's legislative authority is divided between the legislative assemblies of the states that form the Union of India and Parliament (the central government). In some matters both have concurrent legislative powers. Section 246 of India's 1950 Constitution makes policing the responsibility of its states (entries 1 and 2 in List II of the Seventh Schedule of India's 1950 Constitution).

Although each of India's states has legislative authority, the structure and practices of the states' police forces either are governed by India's Police Act 1861 or use that Act to provide the model for their own police procedure manuals. That Act, together with the operation of other legislation, such as

the Indian Penal Code 1860, the Indian Evidence Act 1873 and the Criminal Procedure Code 1973 (which replaced the Criminal Procedure Code 1861), apply throughout India, imposing uniformity on Indian policing.

From time to time special laws to combat terrorism have been enacted in India. The Terrorist and Disruptive Activities Prevention Act (TADA) was in use for quite a few years. However, strong and vociferous criticism about its draconian provisions and misuse in some cases led to it being repealed. The Prevention of Terrorists Activities Act (POTA) was introduced in its place, but that Act is also no longer in force, and there is now no special law to deal with terrorist activities in India.

Policing and security organizations

India's state police organizations are headed by Director-Generals/Inspector-Generals of police, accountable to the relevant state government for the administration and good order of the state's police.

Unfortunately, even after Independence (1947), the original hierarchical police structure in India has remained substantially intact, and no serious attempt has been made to redefine the relationship between the police and the government so as to better reflect the needs of a democracy. In particular, it needs to be made clear that the police are not simply an instrument of the executive arm of government – and, as such, highly susceptible to corruption – but are rather servants of the law and protectors of the rights of the ordinary citizenry.

Numerous commentators and commissions of inquiry have made this point, including the Kerala Police Commission (1959), the National Police Commission (1981) and the National Commission to Review the Working of the Constitution of India (2002). The National Police Commission, for example, recommended that the investigative wing of the police needed to be insulated from external pressures and that the head of the police be given statutory tenure.

Each state has a Criminal Investigation Department (CID). The CIDs are divided into two cohorts, the Crime and the Intelligence branches. Each of these CID branches is headed by an Inspector-General or an Additional-Inspector-General.

In the "Company" era, some of India's great cities (Calcutta, Madras, Bombay) modelled the police of London rather than the paramilitary forces of the British colonies. Such police forces were commanded by a Commissioner of Police who was accountable not to the state government via an Inspector-General but directly to the local city government. Police Commissioners enjoyed judicial-

executive authority and licensing and regulatory powers that elsewhere lay within the purview of District Magistrates. In modern India, larger cities or developmental areas with special needs have established Commissionerates.

Thus Cyberabad Commissionerate is located in India's ''Silicon Valley'', the home of its burgeoning IT industry. This go-ahead Commissionerate is conducting a community-interactive Culture Change Management Programme, a staple of which is ''constabulary empowerment'', intended to overcome the limitations of an ''officer-centered'' orientation imposed by the 1861 Police Act. Constables have been retitled constable officers, and up-skilled as problem-solving ''police executives'', with ownership of and responsibility for the execution of solutions to policing problems, including the use of IT.

The central government's responsibility under the Constitution includes protecting states against internal disturbances, guarding India's 14,090 km land border, providing security for infrastructure and the like.

As well as ''communalism'' (inter-communal violence) and foreign invasion (China in 1962 and Pakistan in 1965), India faces cross-border terrorist incursions and its own internal terrorism, including: (a) leftist extremism (Naxalism) in the states of Andhra Pradesh, Maharashtra, Chattisgarh, Jharkhand, Bihar, Madhya Pradesh, Orissa and West Bengal; (b) ethnic extremism in Nagaland, Tripura, Assam and Arunachal Pradesh in furtherance of demands for seccession from India; and (c) religious extremism in Kashmir, where the Muslim majority variously seek the freedom (Azadi) of an independent Kashmir state, or unification with Pakistan. In recent years Kashmir-based terrorist groups, notably Lashkar-e-Toiba, have undertaken terrorist attacks in Indian cities outside Kashmir, such as Mumbai and Delhi. Moreover, although the majority of the population of India still do not possess computers, mobile phones and the like, there has nevertheless been an exponential growth in the use of communication and information technology and, as a consequence, a steady increase in cybercrime. Among other things, the Indian government is concerned about cyber-terrorism, cyber-warfare and transnational crime involving the use of communication and information technology.

The central government's Minister for Home Affairs has a coordinating function, and may deploy central government police assets to assist states. Such central government police asset forces as have been deployed lifted Indian police numbers to 1.8 million and include: the Central Reserve Police Force (CRPF); the Border Security Force (BSF); the Indo-Tibetan Border Police (ITBP); the Central Industrial Security Force (CISF); and the Railway Protection Force (RPF).

Central government organizations concerned with intelligence and investigation include: the Central Intelligence Bureau (CIB) (which focuses on domestic

intelligence); the Research and Analysis Wing (RAW) (which focuses on external intelligence, e.g. regarding India's conflict with Pakistan); the Central Bureau of Investigation (CBI); the National Investigation Agency (NIA); and the National Crime Records Bureau (NCRB). Other central government agencies include the Bureau of Police Research and Development and the Institute of Criminology and Forensic Science.

Privacy and information technology

In India, the right to privacy derives from the Constitution as well as the common law of torts. The Constitution does not explicitly recognize the right to privacy but, as mentioned earlier, Article 21 provides for personal liberty, and in various cases this has been taken by the Supreme Court to include the right to privacy against the state.[7] For example, in *Kharak Singh v State of Uttar Pradesh* (1964) the Supreme Court held that police intrusions into a person's house were a violation of privacy. In *People's Union for Civil Liberties v. Union of India* 1997, the Supreme Court held that telephone tapping by the government under the Telegraph Act 1885 constituted an infringement of privacy. On the other hand, in the course of these judgments it emerged that the right to privacy is not absolute and can be lawfully infringed for the prevention of crime and disorder. So telephone tapping on the part of law enforcement agencies is permissible under certain conditions.

In India, there is no right against infringements of privacy by individuals or other private entities. Nevertheless, individual or other private entities who infringe one's privacy are subject to the common law of torts and are liable for damages. That said, there is no privacy protection authority in India.

Data protection is not explicitly provided for in the Constitution and, under its right in the Constitution to legislate in relation to matters not enumerated in the relevant lists, the central government has taken it to be an appropriate matter for its involvement. Accordingly, it has enacted the Information Technology Act 2000. The Act declared computers and computer networks to be protected systems and provided for various civil and criminal offenses in respect of unauthorized computer access, theft of computer data, destruction of data, corruption of data, fraud and so forth. The Act also set up various regulatory authorities, such as the Cyber Regulations Appellate Tribunal. However, there is no data protection authority in India. On the other hand, computerization has a long way to go in India, including among law enforcement agencies, and there are few comprehensive electronic data bases of a kind that would enable efficient and effective data mining or profiling.

7 This also enables India to partially fulfil its international obligations under the International Covenant on Civil and Political Rights, in which a basic right to privacy is recognized.

In 2009 the Information Technology (Amendment) Act 2008 was enacted in part to address not only domestic and regional security issues, including cyber-crimes and cyber-terrorism, but also, and very importantly, the security concerns of foreign companies in respect of India's huge outsourcing industry. The Act provides penalties for various new cyber-crimes (e.g. cyber-terrorism and identity theft), the recognition of new electronic documents (e.g. electronic documents with e-signatures) and enhanced data security (e.g. for intermediaries (any person who receives, stores or transmits data for another person such as internet service providers)).

In 2007, the Indian IT software and services industry generated export revenues of US$31.3 billion (especially from the US and EU) and it is projected to increase this to US$60 billion in 2010.[8] Approximately 80% of the world's 500 largest companies outsource some of their sales calls, technical help desks, payroll management and/or legal services etc. to India.[9]

As already noted, data security is not simply a general concern, it constitutes a specific threat to India's billion-dollar IT outsourcing industry and, as a consequence, the Indian government and the Indian IT industry have joined forces with respect to legislation and on several other fronts to deal with the data security issue. The Information Technology (Amendment) Act 2008 is part of the legislative response. The establishment by NASSCOM of the Data Security Council of India (DSCI) is part of the broader institutional response – in this instance, a self-regulatory part, for the DSCI represents software companies and the business process outsourcing (BPO) and related IT industries. The function of DSCI is to establish, disseminate, monitor and enforce privacy and data protection standards for India's IT and outsourcing industry. Obviously, enforcement is the key challenge for DSCI; however, it is difficult to see how what is essentially a voluntary organization can effectively enforce the standards it establishes other than by the threat of expulsion.

The Information Technology Act 2000 and the Information Technology (Amendment) Act 2008 do not set out a comprehensive set of specific privacy and data protection principles in the manner of, say, the EU Directive or the OECD Guidelines. Rather, they require the use of ''reasonable security practices and procedures'', defined in terms of practices and procedures designed to protect sensitive personal information from unauthorized access, damage, use, modification, disclosure etc. However, the DSCI has recommended that companies implement one of the available industry-recognized standards such as the OECD

8 N. Saravade (former Director of Cyber Security and Compliance, National Association of Software and Service Companies (NASSCOM)), available at: http://nationalskillsregistry.com/winwin.html.)

9 See: http:www.reuters.com/article/idUSSP4999820060207.

Privacy Principles for Information Management Systems. Nevertheless, there is no requirement that companies undergo an audit to verify the existence and efficacy of the controls they have in place to meet any such industry standards.

The Indian government and, specifically, the Department of Information Technology (DIT) within the Ministry of Communication and Information Technology, has embarked on an ambitious program of e-governance known as the National eGovernance Program (NeGP) in relation to the delivery of citizen services at both central and state government levels. This program faces prodigious challenges in terms of resources, skill levels of personnel and IT infrastructure and equipment, although more so in some states than in others. The implementation of such an e-governance program in the Indian social and institutional context brings with it multiple security threats. Recognizing the vulnerability of the information infrastructure to e-crime and e-corruption, the government has formulated an information security policy, established various bodies (notably the Computer Emergency Response Team (CERT-In) within the DIT) and required that the government's information infrastructure be subjected to an annual audit. However, the focus of this audit is principally on the technical IT systems and networks.

Agencies

Central Bureau of Investigation (CBI)

The CBI is a central government agency and India's leading investigative agency. The CBI's remit is very wide and includes criminal offenses, corruption and national security matters. It can investigate offenses anywhere in India. The authority of investigation of the CBI can be exercised only on a specific case-by-case authorization by the concerned state government or High Court.

Its power to investigate derives from the Delhi Special Police Establishment Act 1946, according to which it can investigate offenses only in the union territories. However, its jurisdiction can be extended by the central government to the states, provided that the state government in question consents.

Cases investigated by the CBI include: those involving employees of the central government or in which a central government organization is involved; breaches of the Official Secrets Act involving the central government; serious breaches of import/export laws; trans-jurisdictional crime; serious fraud; and organized crime.

The Director of the CBI is a Director General of Police within the Delhi Special Police Establishment. Although the CBI is an administrative unit of the Ministry of Home Affairs, in operational and policy terms the CBI is controlled by the

Department of Personnel and Training under a Minister of State who reports to the Prime Minister. However, the investigation by the CBI of offenses under the Prevention of Corruption Act 1988 (involving offenses by public officials of the central government) are controlled by the Central Vigilance Commission (CVC). The CVC also oversees the CBI.

Central Vigilance Commission (CVC)

The CVC is a statutory body established under the Central Vigilance Commission Act 2003. It consists of a Central Vigilance Commissioner and two Vigilance Commissioners. Its principal focus is corruption within central government agencies. It identifies high-risk areas, conducts surprise inspections to detect system deficiencies and malpractices and advises in relation to, and monitors the workings of, anti-corruption systems. It also receives written complaints on any allegation of corruption or misuse of office and recommends appropriate action. It does not act on anonymous complaints. However, the identity of the complainant is not revealed and the CVC can direct the relevant authorities to provide protection to complainants.

The CVC is not an investigative agency. Rather, as noted above, it initiates and supervises corruption investigations carried out by the CBI or by departmentally based vigilance (anti-corruption) officers. An exception is the investigation by the CVC of civil works/contracts (e.g. scrutiny of financial controls, reasonableness of prices, tender documents, purchase manuals, filing systems etc.), conducted by the Chief Technical Examiners Organization, which is the Technical Wing of the CVC.

The CVC has undertaken a number of new initiatives including naming corrupt officials on its website (''naming and shaming''), and enhancing transparency in high-risk areas such as procurement by the use of new information technology processes, for example, e-bidding and e-payment.

Intelligence Bureau (IB)

The IB has an intelligence-gathering and an assessment function. It also has a preventive function, for example, in developing security checks, vetting procedures and the like. The IB is focused on internal security, including public order, terrorism, sabotage of vital installations, VIP security and counter-intelligence, and it is an administrative unit of the Ministry of Home Affairs. However, the Director of IB is a member of the Joint Intelligence Committee (which is in turn responsible to the Cabinet Secretariat in the Prime Minister's Office) and has the authority to brief the Prime Minister should the need arise. The IB operates at both central and state levels (through state IBs). However, as noted above, the internal security situation in many states is precarious.

In the interest of national security, the IB's intelligence-gathering operations include human intelligence (e.g. from informants, mail and telephone interception). Moreover, in the interest of national security, the central government – and, therefore, the IB – has the authority to intercept, monitor and block access to electronic information and to monitor and collect data identifying a person, computer system or location to or from which the communication was transmitted.

Infringements of human rights on the part of law enforcement and intelligence agencies, including the IB, can be investigated by the National Commission on Human Rights. However, it is unclear what specific oversight mechanisms there are in relation to the IB.

Research and Analysis Wing (RAW)

RAW is India's foreign intelligence agency. RAW has intelligence-gathering, counter-intelligence and assessment functions. It also engages in covert operations, for example, covert assistance to the ANC, training members of Liberation Tigers of Tamil Eelam and attempts to limit the supply of military hardware to Pakistan. Although its personnel and their numbers are shrouded in secrecy, it is estimated to employ around 10,000 agents.[10]

The head of RAW is the Secretary (Research) in the Cabinet Secretariat, which is part of the Prime Minister's Office. In relation to operational matters the Secretary (Research) reports to the National Security Advisor. In addition to its headquarters in Delhi, RAW has a number of regional offices and various overseas stations.

Infringements of human rights on the part of law enforcement and intelligence agencies, including RAW, can be investigated by the National Commission on Human Rights. However, the activities of RAW are highly secretive and it is unclear what specific oversight mechanisms exist in relation to RAW.

10 "RAW: India's External Intelligence Agency", Council on Foreign Relations, available at: http:www.dfr.org/publications/17707/.