

CHAPTER 8: COMPARATIVE LAW ¹

8.1 Introduction

8.1.1 It is important to learn from the experiences of other countries. In conducting comparative research it would, however, be dangerous to translate the experiences of other countries directly into your own law. Key areas of possible divergence which may have an influence on the data

1

Unless otherwise indicated, the information reflected in this chapter is based on extracts from the Country Reports in Electronic Privacy Information Center (EPIC) in association with Privacy International *Privacy and Human Rights 2003: An International Survey of Privacy Laws and Developments* as updated in *Privacy and Human Rights 2004: An International Survey of Privacy Laws and Developments* and the references therein. This annual report published in the USA by EPIC and Privacy International, reviews the state of privacy in over sixty countries around the world. It outlines legal protections for privacy, new challenges, and summarises important issues and events relating to privacy and surveillance. Electronic versions of the report is available at <http://www.privacyinternational.org/>. See also <http://www.epic.org/>.

privacy model to be chosen may, for instance, include:²

- the legal framework and the protection afforded to data privacy;³

2

A Performance and Innovation Unit of the UK Cabinet Office *Privacy and Data-Sharing: The Way Forward for Public Services* Ann B, International Comparisons April 2002 (hereafter referred to as "*PIU Privacy and Data Sharing Report*") at 18.

3

Some countries may have a common law jurisdiction, as opposed to civil law elsewhere. Federal countries laws, standards or targets at the national level may differ from those covering provinces or regions. Overall frameworks may differ. While the US data protection law gives less protection to the citizen than EU laws, there is a specific tort of privacy, through which US citizens are able to sue in respect of breach of their privacy.

- cultural attitudes to openness and privacy and the role of the government;⁴
- historical events, which may have left an indelible impression on public attitudes to privacy;⁵ and
- population size, which has an impact on the ease with which projects can be implemented.⁶

8.1.2 Even taking into account these influences, it is clear that there has been a harmonisation in the implementation of information protection principles and that the international nature of these principles has already promoted, and will also in future promote, the development of global standards.

4 In Sweden it is accepted that everyone's tax return can be inspected by anyone who cares to do so. Similarly, in many countries it is accepted that drivers should carry their licence with them at all times, whereas it is a hotly debated topic in some other countries.

5 Dutch government files listing religious affiliation were used by the Nazis to identify Jews. So a reasonably innocent proposal concerning information on religion may nevertheless touch a nerve there.

6 If a country already has a national ID card, it is relatively straightforward to issue a smart card version with functionality for public key cryptography. In the absence of such a pre-existing framework, however, options are more limited.

8.2 International Directives⁷

8.2.1 The first data protection laws in the world were enacted in the seventies.⁸ There are now well over thirty countries which have enacted data protection statutes at national or federal level and the number of such countries is steadily growing.⁹

8.2.2 Important international instruments evolved from these laws, most notably the Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data¹⁰ and the 1981 Organisation for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.¹¹

8.2.3 These two agreements have had a profound effect on the enactment of laws around the world. Nearly thirty countries have signed the COE convention. The OECD guidelines have also

⁷ See discussion with regard to international instruments in paras 1.2.12 and 4.1 above.

⁸ An analysis of these laws is found in Flaherty D *Protecting Privacy in Surveillance Societies* University of North Carolina Press 1989.

⁹ Bygrave *Data Protection* at 30.

¹⁰ Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, ETS No. 108, Strasbourg, 1981.

¹¹ OECD Guidelines.

been widely used in national legislation, even outside the OECD member countries.

8.2.4 The Convention is the hereto sole international treaty dealing specifically with data protection. It entered into force on 1 October 1985.¹² The Convention is potentially open for ratification by States that are not members of the CoE;¹³ concomitantly it is also envisaged to be potentially more than an agreement between European states. As yet, though it has not been ratified by any non-member states.¹⁴

8.2.5 The Convention is not intended to be self-executing. Art 4(10) of the Convention simply obliges Contracting States to incorporate the Convention's principles into their domestic legislation; individual rights cannot be derived from it.¹⁵

8.2.6 The OECD Guidelines incorporate eight principles relating to the collection, purpose, use, quality, security and accountability of organisations in relation to personal information. However, the OECD Guidelines do not set out requirements as to how these principles are to be enforced by member nations. As a result, OECD member countries have chosen a range of differing measures to implement the privacy principles.

8.2.7 In 1995, the European Union enacted the Data Protection Directive¹⁶ in order to harmonise member states' laws in providing consistent levels of protection for citizens and ensuring the free flow of personal data within the European Union.

8.2.8 Articles 25 and 26 of the Directive stipulates that personal data should only flow outside the boundaries of the Union to countries that can guarantee an "adequate level of protection" (the so-

12 EPIC and Privacy International *Privacy and Human Rights Report 2003* at 9. It has been ratified by 30 CoE Member states.

13 Art 23.

14 Bygrave *Data Protection* at 32.

15 Bygrave *Data Protection* at 34.

16 EU Directive.

called safe-harbour principles).¹⁷

17

For further discussion see Ch 7 above.

8.2.9 The Directive sets a baseline common level of privacy that not only reinforces current data protection law, but also establishes a range of new rights. The Directive contains strengthened protections over the use of sensitive personal data relating, for example, to health, sex life or religious or philosophical beliefs. In future, the commercial and government use of such information will generally require “explicit and unambiguous” consent of the data subject. The directive applies to the processing of personal information in electronic and manual files.¹⁸ It provides only a basic framework which will require to be developed in national laws.¹⁹

8.2.10 The Directive was adopted with member states being required to implement its provisions by October 24, 1998. This time-table has proven difficult for Member States to comply with.

8.2.11 Some account should also be taken of the UN Guidelines.²⁰ The Guidelines are intended to encourage those UN Member States without information protection legislation in place to take steps to enact such legislation based on the Guidelines. The Guidelines are also aimed at encouraging governmental and non-governmental international organisations to process personal information in a responsible, fair and privacy-friendly manner. The Guidelines are not legally binding and seem to have had much less influence on information regimes than the other instruments.²¹

18 See Ch 1 above.

19 As referred to in Strathclyde LLM at 4. A good example is the Directive’s requirement that member states shall appoint an independent supervisory agency. The particular form of the agency is not specified.

20 UN Guidelines.

21 Bygrave *Data Protection* at 33.

8.2.12 The Commonwealth Law Ministers have furthermore proposed for consideration by Senior Officials at their meeting in November 2001 that model legislation (Model Bills) to implement the Commonwealth commitment to freedom of information should be enacted for both the public and the private sectors.

8.2.13 The intent of the proposed model legislation is to ensure that governments and private organisations accord personal information an appropriate measure of protection, and also that such information is collected only for appropriate purposes and by appropriate means. The model seeks, in accordance with general practice in member countries only to deal with information privacy which is the most common aspect of privacy regulated by statute and which involves the establishment of rules governing the collection and handling of personal information such as those relating to status of credit or medical records. It also seeks to create a legal regime which can be administered by small and developing countries without the need to create significant new structures.²²

8.2.14 In February 2003, Australia put forward a proposal for the development of APEC (Asia-Pacific Economic Cooperation) Privacy Principles, using the OECD Guidelines as a starting point.²³ In March 2004, version 9 of the APEC Privacy Principles was released as a public consultation draft. Implementation mechanisms, including mechanisms to deal with transborder data flows are also still under consideration. A high APEC standard could be a means of resolving international data export issues, but low standards could result in a privacy confrontation between Europe and the Asia-Pacific.²⁴

8.2.15 Although the expression of data protection in various declarations and laws varies, all require that personal information must be:

²² The Meeting considered both Model Laws. The Law Ministers commended the Model law for the public sector as a useful tool which could be adopted to meet the particular constitutional and legal positions in member countries. They decided, however, that the Model Bill on the Protection of Personal Information needed more reflection. They asked the Commonwealth Secretariat to prepare an amended draft which would be considered at the next planning meeting of Secretariat officials.

²³ A Privacy Sub Group was set up comprising Australia, Canada, China, Hong Kong, Japan, Korea, Malaysia, New Zealand, Thailand and the United States.

²⁴ EPIC and Privacy International *Privacy and Human Rights Report 2004* and the references made therein.

- obtained fairly and lawfully;
- used only for the original specified purpose;
- adequate, relevant and not excessive to purpose;
- accurate and up to date;
- accessible to the subject;
- kept secure; and
- destroyed after its purpose is completed.

These principles are known as the “Principles of Data Protection” and form the basis of both legislative regulation and self-regulating control.

8.3 United States of America²⁵

8.3.1 The United States Constitution does not explicitly mention a right to privacy. The Supreme Court has, however, ruled that there is a limited constitutional right of privacy based on a number of provisions in the Bill of Rights. This includes a right to privacy from government surveillance into an area where a person has a “reasonable expectation of privacy”²⁶ and also in so far as marriage, procreation, contraception, family relationships, child rearing and education are concerned.²⁷

8.3.2 Two characteristics of American constitutional law should be kept in mind: Firstly, Constitutional rights are usually not applicable unless “state action” can be found. This means that the rights created by the Constitution protect the individual from the government and not from private entities. Secondly, the rights created by the Constitution are “negative rights” - they prevent certain kinds of governmental action, but place no affirmative duties on the state to protect the constitutional rights of individuals by actions such as the adoption of legislation. There is, therefore, no duty on the government to actively protect an individual against the invasion of his or her

²⁵ EPIC and Privacy International *Privacy and Human Rights Report 2003* at 522 and the references made therein. See also the discussion regarding the self-regulatory system of the USA in para 5.3.43-46 in Ch 5 above.

²⁶ *Katz v United States* 386 U.S. 954 (1967).

²⁷ See e.g., *Griswold v Connecticut*, 381 U.S. 479 (1965); *Whalen v Roe* 429 United States 589 (1977); *Paul v Davis* 424 U.S. 714 (1976).

informational privacy rights.²⁸

28

Roos thesis at 38 and the references made therein.

8.3.3 The Privacy Act of 1974 regulates the information practices of federal agencies.²⁹ It requires agencies to apply basic fair information procedures.³⁰ The efficiency of the Act is, however, hampered by a weak remedial scheme and the lack of a proper information protection authority. It has furthermore been argued³¹ that its effectiveness is significantly weakened by administrative interpretations of a provision allowing for disclosure of personal information for a “routine use” compatible with the purpose for which the information was originally collected. Limits on the use of the Social Security Number have also been undercut in recent years because Congress has approved new purposes for the identifier and because the private sector employs the identifier for many purposes with virtually no safeguards for the individual.

8.3.4 In the 2003 term, the Supreme Court considered the Privacy Act, a privacy exemption to the Freedom of Information Act, and the issue of whether police could compel an individual to identify himself in public. In *Doe v. Chao*,³² the Court ruled that a plaintiff in a Privacy Act suit must demonstrate actual damages to qualify for the Act's minimum statutory award of USD 1,000.³³

²⁹ See also the Family Educational Rights and Privacy Act (FERPA) Pub L 93-380, 88 Stat 571 (1974); Right to Financial Privacy (RFPA) 1978 Pub L 95-630; Privacy Protection Act (PPA) Pub L 96-440 codified at 42 USC s2000aa; Health Insurance Portability and Accountability Act (HIPAA) Pub L 104-191 codified at 42 USCA s 1320.; etc.

³⁰ Privacy Act, Pub. L. No. 93-579 (1974), codified at 5 USC § 552a,.

³¹ EPIC and Privacy International *Privacy and Human Rights Report 2003* at 524.

³² 124 S.Ct 1204 (2004).

³³ EPIC and Privacy International *Privacy and Human Rights Report 2004* and the references made therein.

8.3.5 In March 2003, the Department of Justice announced that it would exempt the National Crime Information Center (NCIC) from data quality standards in the Privacy Act. The NCIC contains 39 million criminal records, and is used by over 80,000 law enforcement agencies. The change was strongly opposed by a broad coalition of organizations and individuals across the United States.³⁴

34

ibid.

8.3.6 The United States has no comprehensive privacy protection law for the private sector. Various federal laws cover some specific categories of personal information. These include financial records,³⁵ credit reports,³⁶ video rentals,³⁷ cable television,³⁸ children's (under age 13) online activities,³⁹ educational records,⁴⁰ motor vehicle registrations,⁴¹ and telemarketing.⁴²

8.3.7 There is no independent information protection agency in the United States. Oversight takes place on different levels, namely by the head of an agency, the Office of Management and Budget, the US President, Congress and the courts:

35 Right to Financial Privacy Act, Pub. L. No. 95-630 (1978).

36 Fair Credit Reporting Act, Pub. L. No. 91-508 (1970), amended by PL 104-208 (1996).

37 Video Privacy Protection Act, Pub. L. No. 100-618 (1988).

38 Cable Privacy Protection Act, Pub. L. No. 98-549 (1984).

39 See Center for Media Education, A Parent's Guide to Online Privacy.

40 Family Educational Rights and Privacy Act, Public Law 93-380, 1974.

41 Drivers Privacy Protection Act, PL 103-322, 1994.

42 Telephone Consumer Protection Act, PL 102-243, 1991.

- The Office of Management and Budget ⁴³plays a limited role in setting policy for federal agencies under the Privacy Act, but it has not been particularly active or effective.
- In 1999 a Chief Counselor for Privacy was appointed within the Office of Management and Budget to coordinate federal stances towards privacy. The Counselor had only a limited advisory capacity. The Bush Administration has eliminated this position.

43

Part of the executive office of the President.

- The Federal Trade Commission has oversight and enforcement powers for the laws protecting children's online privacy, consumer credit information and fair trading practices but has no general authority to enforce privacy rights. The FTC has received thousands of complaints but has issued opinions in only a few cases. It has also organised a series of workshops and surveys, which have found that industry protection of privacy on the Internet is poor, but the FTC had long said that the industry should have more time to make self-regulation work. In a shift from this position, in June 2000, the FTC recommended in a report to the United States Congress that legislation is necessary to protect consumer privacy on the Internet due to the dismal findings in a survey of online privacy policies.⁴⁴ Since issuing that report, the new Chairman of the Commission appointed by President Bush has recommended that more study is necessary before legislation is passed to protect Internet Privacy.⁴⁵ Instead, FTC has focused on enforcing existing law in the areas of telemarketing, spam, pretexting, and children's privacy.⁴⁶ In January 2002, the FTC proposed changes to the Telemarketing Sales Rule to tighten use of individuals' account numbers, and to create a national do-not-call list for individuals who wish to opt-out of telemarketing.⁴⁷ Enrolment began in June 2003, and now approximately 60 million numbers have been added to the list.⁴⁸

8.3.8 Since article 25 of the EU Directive prohibits the transfer of personal information from EU countries to third countries without adequate information protection, fears were raised in the USA that the free flow of information between the US and Europe would be hampered. A safe-harbour agreement was subsequently negotiated in 2002 which consists of a set of information principles agreed upon by the USA and the European Commission with which all parties have to comply

44 ***Privacy Online: Fair Information Practices in the Electronic Marketplace***: A Federal Trade Commission Report to Congress May 2000.

45 Protecting Consumers' Privacy: 2002 and Beyond, Remarks of FTC Chairman Timothy J. Muris, October 2001.

46 See FTC Privacy Initiatives.

47 The Proposed National "DO NOT CALL" Registry, Amendment to the Telemarketing Sales Rule, January 2002.

48 EPIC and Privacy International ***Privacy and Human Rights Report 2004*** and the references made therein.

voluntarily.⁴⁹

8.3.9 Developments since 1999 have been as follows:

- The end of 1999 brought increased scrutiny on financial privacy. In 1999, the Michigan Attorney General sued several banks for revealing that they were selling information about their customers to marketers. Other banks across the country subsequently admitted that they were also selling customer records. The Gramm-Leach-Bliley Act, which eliminated traditional ownership barriers between different financial institutions such as banks, securities firms and insurance companies, set limited protections on financial information that is likely to be shared among merged institutions. The effective date of the privacy provisions were pushed back from November 2000 until July 2001.

49

See discussion in Ch 7 above.

- In 2000 the sole federal law governing information use online went into effect. The Children's Online Privacy Protection Act (COPPA), passed by Congress in 1998 and requiring parental consent before information is collected from children under the age of 13, went into effect in April 2000.⁵⁰

- Protections for medical records were introduced in the United States in 2001. In October 1999, the Department of Health and Human Services issued draft regulations protecting medical privacy. The final rules were issued on December 20, 2000 and went into effect in April 2001. The large number of exemptions provided limits to the protection offered by the new rules. For example, patients' information can be used for marketing and fundraising purposes. Doctors, hospitals, and health services companies will be able to send targeted health information and product promotions to individual patients and there is no opt-out right to limit this marketing use of medical data.⁵¹ In April 2003, the first federal regulation protecting individually identifiable health information became effective for enforcement. The Standards for Privacy of Individually Identifiable Health Information, commonly known as the "HIPAA Privacy Rule," provide basic protections for individually identifiable health information and give individuals rights with respect to the information about them.⁵² The federal Privacy Rule contains civil penalties for non-compliance and will be enforced by the Office for Civil Rights within the Department

50 FTC Privacy Pages .

51 Office of the Secretary ***Standards for Privacy of Individually Identifiable Health Information***; Proposed Rule 45 CFR Parts 160 and 164, §164.501 March 27, 2002.

52 EPIC and Privacy International ***Privacy and Human Rights Report 2004*** and the references made therein.

of Health and Human Services. The Rule also contains criminal penalties for malicious misappropriation and misuse of health information, which will be enforced by the Department of Justice.⁵³

53

EPIC and Privacy International *Privacy and Human Rights Report 2004* and the reference made to EPIC's Medical Privacy web page available at <http://www.epic.org/privacy/medical/>.

- In 2003, Congress passed legislation significantly amending the Fair Credit Reporting Act (FRCA) and the nation's first spam regulation.⁵⁴

8.3.10 There is also a variety of sectoral legislation on the state level that may give additional protection to citizens of individual states. The tort of breach of privacy was first adopted in 1905 and all but two of the 50 states recognise a civil right of action for invasion of privacy in their laws.⁵⁵ A number of court cases have dealt with the protection of the right to privacy and data.⁵⁶

54 EPIC Fair Credit Reporting Act page available at <http://www.epic.org/privacy/frca/>.

55 See *Lake v WalMart Stores, Inc.*, 582 N.W.2d 231 (Minn. 1998), for a review of state adoption of common law privacy torts.

56 See discussion of the following cases in EPIC and Privacy International *Privacy and Human Rights Report 2003* at 522: In January 2000, the Supreme Court heard *Reno v Condon*, 528 U.S. 141 (2000), a case addressing the constitutionality of the Drivers Privacy Protection Act (DPPA), a 1994 law that protects drivers' records held by state motor vehicle agencies. In a unanimous decision, the Court found that the information was "an article of commerce" and can be regulated by the federal government. In June 2001, the Supreme Court ruled in the case of *Kyllo v United States* 533 U.S. 27 (2001) that the use of a thermal imaging device, without a warrant, to detect heat emanating from a person's

residence constituted an illegal search under the Fourth Amendment.¹⁹⁶¹ *City of Indianapolis v Edmond*, 531 U.S. 32 (2000). In November 2000, the Supreme Court ruled held that suspicionless vehicle checkpoints, used to discover and interdict illegal narcotics, violate the Fourth Amendment.¹⁹⁶² Also, in March 2001, the Supreme Court held that a state hospital cannot perform diagnostic tests to obtain evidence of criminal conduct without the patient's consent as such a test is unreasonable and violates the Fourth Amendment. *Ferguson v City of Charlestown*, 532 U.S. 67 (2000). In the 2001 term, the Supreme Court addressed anonymity, searches on buses, and student privacy. In *Watchtower Bible*, the Court invalidated a law that required registration with the government before individuals could engage in door-to-door solicitation. The Court held that a pre-registration requirement violated the First Amendment and individuals' right to anonymity. *Watchtower Bible & Tract Soc'y of N.Y. v. Village of Stratton*, 122 S. Ct. 2080 (2002). In *United States v Drayton*, the Court held that the Fourth Amendment does not require police officers to advise bus passengers of their right not to cooperate and to refuse consent to searches. *United States v Drayton*, 122 S. Ct. 2105 (2002). Student privacy was diminished in a series of cases involving drug testing, "peer grading," the practice of allowing a fellow student to score a test, and the right to sue under a federal student privacy law. In *Earls*, the Court held that random, suspicionless drug testing of students involved in non-athletic extracurricular activities was justified under the "special needs" exception to the Fourth Amendment. Bd. of *Educ. v Earls*, 122 S. Ct. 2559 (2002). In *Falvo*, the Court held that both peer grading and the reporting aloud of peer grades did not violate the Family Educational Rights and Privacy Act of

8.3.11 There has been significant debate in the United States in recent years about the development of privacy laws covering the private sector.⁵⁷

- a) The **White House and the private sector** maintain that self-regulation is sufficient and that no new laws should be enacted except for a limited measure on medical and genetic information.

1974 (FERPA). *Owasso Indep. Sch. Dist. No. I-011 v Falvo*, 534 U.S. 426 (2001). In *Gonzaga*, the Court held that the FERPA does not give individuals a right to sue for violations of privacy *Gonzaga Univ. v Doe*, 122 S. Ct. 2268 (2002).

57

EPIC and Privacy International *Privacy and Human Rights Report 2003* at 529 and the references as indicated below.

- b) There have been many **efforts in Congress** to improve privacy. Since January 2001, there have been well over 100 bills introduced in the House and Senate.⁵⁸
- c) There is also **substantial activity in the states**. In recent years, Massachusetts and Hawaii have considered comprehensive privacy bills for the private sector. California passed a Social Security Number Bill that will prevent the printing of the identifier on forms, invoices, and identification badges. The Bill also gives individuals greater power to control their credit report once fraud is suspected.⁵⁹ Minnesota enacted a Bill that requires ISPs to give notice and obtain user authorisation before using personal information for secondary purposes.⁶⁰ In a statewide referendum, North Dakota residents established opt-in protections for financial information.⁶¹ Additionally, Georgia enacted a privacy law that prohibits private businesses from discarding documents or computer components that contain personal information⁶².
- d) **Internet privacy** has remained the hottest issue of the past few years. A number of

58 See EPIC Bill Track.

59 California Senate Bill 168.

60 Minnesota S.F. 2908.

61 Friery T "Privacy Alert: North Dakota Votes for 'Opt-In' Financial Privacy," Privacy Rights Clearinghouse, June 21, 2002.

62 Georgia Senate Bill 475.

profitable companies, including eBay.com, Amazon.com, drkoop.com, and yahoo.com have either changed users' privacy settings or have changed privacy policies to the detriment of users.⁶³ A series of companies, including Intel and Microsoft, were discovered to have released products that secretly track the activities of Internet users.⁶⁴ Users have filed several lawsuits under the wiretap and computer crime laws. In several cases, TRUSTe, an industry-sponsored self-regulation watchdog group ruled that the practices did not violate its privacy seal program.

63 Hoofnagle CJ *Consumer Privacy In the E-Commerce Marketplace 2002* Third Annual Institute on Privacy Law Practicing Law Institute G0-00W2 (June 2002).

64 See Big Brother Inside Campaign .

- e) Additionally, an **official Homeland Security Agency**⁶⁵ has been created and private-sector corporations are collaborating to use commercial marketing data for terrorism profiling.⁶⁶
- f) Recent years have seen a new trend towards the increased use of **video surveillance** cameras linked with facial recognition software in public places.^{67 68}

65 H.R. 5005, Homeland Security Act of 2002.

66 See Letter from the Center for Information Policy Leadership to Interested Parties, 2002.

67 O'Harrow R "Matching Faces with Mugshots: Software for Police, Others Stir Privacy Concerns," *Washington Post*, July 31, 2001 at A1. See also EPIC's page on Face Recognition.

- g) There have been a number of proposals to create a **National ID**⁶⁹ in the wake of the September terrorist attacks.⁷⁰ Most of these efforts have sought the creation of a national identification system through the standardisation of state driver's

68

This kind of technology was first used at the 2001 Super Bowl in Tampa, Florida to compare the faces of attendees to faces in a database of mug shots. Public usage of the technology then spread to the Ybor City district of Tampa, where the technology encountered much public opposition. In August 2001, the Tampa City Council held a vote on whether they should terminate their contract with Visionics, but they narrowly decided to keep using the software. Virginia Beach, Virginia, received funding in 2001 from the Virginia Department of Criminal Justice Services to install a system that can scan and process the facial images of tourists visiting the town. Face recognition technology is still not reliable and remain unregulated by United States laws. Studies sponsored by the Defense Department have also shown the system is right only 54% of the time and can be significantly compromised by changes in lighting, weight, hair, sunglasses, subject cooperation, and other factors. Declan McCullagh and Robert Zarate, "Scanning Tech a Blurry Picture", *Wired News*, February 16, 2002;. Tests on the face recognition systems in operation at Palm Beach Airport in Florida, American Civil Liberties Union Press Release, "Data on Face-Recognition Test at Palm Beach Airport Further Demonstrates Systems' Fatal Flaws," May 14, 2002,; and Boston Logan Airport have also shown the technology to be ineffective and error-ridden. Hiawatha Bray, "'Face Testing' at Logan is Found Lacking," *Boston Globe*, July 17, 2002.

69

See also the recommendations of the National Commission on Terror Attacks Upon the United States (911 Commission) regarding the need for secure identification in the US.

70

Kent SY and Millett L I *IDs -- Not That Easy: Questions About Nationwide Identity Systems* Editors, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, 2002.

licenses.^{71 72}

71

Your Papers Please: From A State Driver's License to a System of National Identification, EPIC Report, February 2002.

72

A bill to create a National ID has been introduced in the House, but a companion bill has yet to be introduced in the Senate. H.R. 4633, the Driver's License Modernization Act of 2002. There are also more limited attempts to create national identification systems through "enhanced visa" documents and "trusted traveler" programs.

- h) Several other programmes have been initiated in the past few years, such as the US-VISIT,⁷³ SEVIS,⁷⁴ CAPPSII,⁷⁵ MATRIX⁷⁶ and TIA⁷⁷ (discontinued).⁷⁸

73 United States Visitor and Immigrant Status Indicator Technology programme which requires visitors to the USA to submit a biometric identifier to the government.

74 Student and Exchange Visitor Information System is an Internet-based system that allows schools to transmit student information to the government for purposes of tracking and monitoring non-immigrant and exchange students.

75 Computer Assisted Passenger Pre-screening System aims to conduct background risk assessments on all air travellers before they fly on commercial airliners. The intention is to link CAPSS II and US-VISIT when both programmes are fully operational.

76 Multi-state Anti-Terrorism Information Exchange is available to law enforcement agents in participating states and combines public and private records from multiple databases with data analysis tools.

77 Total Information Awareness was a programme of the Defence Advanced Research Projects Agency (DARPA) that intended to scan ultra-large databases of personal information to detect the "information signature" of terrorists.

78 EPIC and Privacy International *Privacy and Human Rights Report 2004* and the references made therein.

8.4 United Kingdom of Great Britain and Northern Ireland⁷⁹

8.4.1 English common law does not recognise the right to privacy and the United Kingdom does not have a written constitution. In 1998, the Parliament approved the Human Rights Act to incorporate the European Convention on Human Rights into domestic law, a process that established an enforceable right of privacy.⁸⁰ The Act came into force on October 2, 2000. A number of cases, many related to celebrity privacy, have been decided or are pending in the courts.

⁷⁹ EPIC and Privacy International *Privacy and Human Rights Report 2003* at 513 and the references made therein.

⁸⁰ Human Rights Bill, CM 3782, October 1997.

8.4.2 The information protection provided by this Act is, however, not significant and protection is therefore provided through specific legislation. The Parliament approved the Data Protection Act in July 1998.⁸¹ The legislation, which came into force on March 1, 2000, replaced the 1984 Data Protection Act. It implements the requirements of the European Union's Data Protection Directive.⁸² The Act covers records held by government agencies and private entities. It provides for limitations on the use of personal information, access to and correction of records and requires that entities that maintain records register with the Information Commissioner.

8.4.3 The Information Commissioner (formerly known as the Data Protection Commissioner and the Data Protection Registrar), is an independent officer that enforces both the Data Protection and Freedom of Information Acts.⁸³ Statistics are published in the Annual Report.⁸⁴ In June 2003, the Commissioner issued a code of guidance for employer/employee relationships.

8.4.4 The Commissioner is also responsible for enforcing the Telecommunications (Data Protection and Privacy) Regulations. These regulations came into force on March 1, 2000, and implement the 1997 European Union Telecommunications Directive.⁸⁵

81 Data Protection Act 1998c. 29.

82 Data Protection Act 1984 (c. 35).

83 Home page of the Information Commissioner, <<http://www.dataprotection.gov.uk/>>.

84 As of March 31, 2002, there were 198,519 databases registered with the Commission.

- a) The agency received 12, 479 requests for assessment and inquiries in 2001-2002.
- b) There were 106 cases forwarded for prosecution resulting in 66 prosecutions and 33 convictions.
- c) The Commissioner has also issued a number of comprehensive reports for the public.
- d) She has published a Code of Practice for the use of Closed Circuit Television (CCTV) and a study of the availability and use of personal information in public registers.

85 Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector. They replaced the Telecommunications (Data Protection and Privacy) (Direct Marketing) Regulations 1998 which came into effect on May 1, 1999.

8.4.5 There are also a number of other laws containing privacy components, most notably those governing medical records⁸⁶ and consumer credit information.⁸⁷ Other laws with privacy components include the Rehabilitation of Offenders Act of 1974, the Telecommunications Act of 1984 (as amended by the Telecommunications Regulations of 1999), the Police Act of 1997, the Broadcasting Act of 1996, Part VI and the Protection from Harassment Act of 1997. Some of these acts are amended and repealed in part by the 1998 Data Protection Act. The Crime and Disorder Act of 1998 provides for information sharing and data matching among public bodies in order to reduce crime and disorder. The Data Protection Commissioner issued a report on the privacy implications of the Act.⁸⁸

⁸⁶ Access to Medical Reports Act 1988, Access to Health Records Act 1990, The Health and Social Care Act 2001.

⁸⁷ Consumer Credit Act, 1974.

⁸⁸ Crime & Disorder Act 1998: Data protection implications for information-sharing.

8.4.6 It has been noted⁸⁹ that the privacy picture in the United Kingdom is mixed. There is, at some levels, a strong public recognition and defence of privacy. Proposals to establish a national identity card, for example, have routinely failed in the past to achieve broad political support. On the other hand, crime and public order laws passed in recent years have placed substantial limitations on numerous rights, including freedom of assembly, privacy, freedom of movement, the right of silence, and freedom of speech.⁹⁰

8.4.7 Home Secretary David Blunkett announced on July 3, 2002 a six month consultation period on “entitlement cards,” a new name for a national ID card proposal.⁹¹ The cards will be mandatory for all persons over 16 years old and would be required to obtain health care, jobs and other services.⁹² A consultation and draft Bill was released in April 2004 . It will require biometric technologies and establish a central National Identity Register.⁹³

8.4.8 The United Kingdom is a member of the Council of Europe and has signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108)⁹⁴ and the European Convention for the Protection of Human Rights and Fundamental Freedoms.⁹⁵ In November 2001, the United Kingdom signed the Council of Europe Convention on Cybercrime.⁹⁶ The United Kingdom is a member of the Organisation for Economic Cooperation and Development and has adopted the OECD Guidelines on the Protection of Privacy and Transborder

89 EPIC and Privacy International *Privacy and Human Rights Report 2003* at 513 and the references made therein.

90 See Criminal Justice and Public Order Act 1994.

91 See Privacy International ID Cards Page.

92 The proposal has been widely criticised by politicians and major media across the political spectrum. Blunkett first proposed the card shortly after September 11 but was forced to back away after it was also severely criticised.

93 EPIC and Privacy International *Privacy and Human Rights Report 2004* and the references made therein.

94 Signed May 14, 1981; Ratified August 26, 1987; Entered into Force December 1, 1987.

95 Signed November 11, 1950; Ratified March 8, 1951; Entered into Force September 3, 1953.

96 Signed November 23, 2001.

Flows of Personal Data.

8.5 Kingdom of the Netherlands⁹⁷

8.5.1 The Dutch Constitution was amended in 1983 to include art 10 which grants citizens an explicit right to privacy.⁹⁸

8.5.2 In May 2000, the government-appointed commission for “Constitutional rights in the digital age” presented proposals for changes to the Dutch constitution. The commission was set up after confusion about the legal status of e-mail under the constitutionally protected privacy of letters. The commission’s task was to investigate if existing constitutional rights should be made more technology-independent and if new rights should be introduced.⁹⁹ No changes have been effected

⁹⁷ EPIC and Privacy International *Privacy and Human Rights Report 2003* at 362 and the references made therein.

⁹⁸ Constitution of the Kingdom of the Netherlands 1989. Article 10 states:
 “(1) Everyone shall have the right to respect for his privacy, without prejudice to restrictions laid down by or pursuant to Act of Parliament.
 (2) Rules to protect privacy shall be laid down by Act of Parliament in connection with the recording and dissemination of personal data.
 (3) Rules concerning the rights of persons to be informed of data recorded concerning them and of the use that is made thereof, and to have such data corrected shall be laid down by Act of Parliament.”

Article 12 states:
 “(1) Entry into a home against the will of the occupant shall be permitted only in the cases laid down by or pursuant to Act of Parliament, by those designated for the purpose by or pursuant to Act of Parliament.
 (2) Prior identification and notice of purpose shall be required in order to enter a home under the preceding paragraph, subject to the exceptions prescribed by Act of Parliament. A written report of the entry shall be issued to the occupant.”

Article 13 states:
 “(1) The privacy of correspondence shall not be violated except, in the cases laid down by Act of Parliament, by order of the courts.
 (2) The privacy of the telephone and telegraph shall not be violated except, in the cases laid down by Act of Parliament, by or with the authorisation of those designated for the purpose by Act of Parliament.”

⁹⁹ According to this proposal, Article 10 will be expanded to the right of persons to be informed about the origin of data recorded about them and the right to correct that data. Article 13 would be made technology-independent and would give the right to confidential communications. Breaches of this right could only be authorised by a judge or a minister. The discussion about possible changes is still ongoing. Data retention requirements and changes to article 13 of the Constitution, as recommended by the Mevis Committee, have recently been officially proposed by the Government in the Telecommunications Data Requisition Bill. In its annual report for 2001, the data protection authority criticised this proposal saying that “constitutional protection should not be restricted to the content of communications, but should extend to ‘traffic data’, i.e. information about the communications.”

yet.

8.5.3 The Wet Bescherming Persoonsgegevens (WBP)(Personal Data Protection Act) of 2000 was approved by the Parliament in June 2000¹⁰⁰. This Act is a revised and expanded version of the 1988 Data Registration Act and brought the Dutch law in line with the European Data Protection Directive. It also regulates the disclosure of personal data to countries outside of the European Union. The sectoral codes of conduct still enjoy a considerable degree of popularity.¹⁰¹ Most of the existing codes are currently under revision for adaptation to the new legislation.

8.5.4 The WBP establishes an independent information protection authority entitled the College Bescherming Persoonsgegevens (CBP) which exercises supervision of the operation of personal data files in accordance with the Act.¹⁰² Previously known as the Registratiekamer, the CBP's functions have remained largely the same with the implementation of the new Act, although it has been given new powers of enforcement. It can now apply administrative measures and impose fines for non compliance with a decision. It can also levy fines of up to 4540 euro for breach of the notification requirements. Otherwise, the CBP continues to advise the government, deal with complaints submitted by data subjects, institute investigations and make recommendations to controllers of personal data files.

8.5.5 A focus of the CBP recently has been on establishing privacy protections within information communication technology. It is a major participant in the European Privacy Incorporated Software Agents (PISA) project¹⁰³ which was established to develop privacy enhancing techniques to protect

100 Personal Data Protection Act, Staatsblad 2000 302, July 6, 2000, unofficial translation.

101 In terms of the now repealed Data Protection Act of 1988 provision was made for the possibility to develop a code of conduct as means of implementation and to request the Data Protection Authority for its approval. The decision of the authority was non-binding, but in practice often seen as a seal of good quality. Under this regime, twelve codes of conduct were officially approved, which covered major sectors like banking and insurance, direct marketing, health and pharmaceutical research. The relevant provision of the Act served as a model for Article 27 of Directive 95/46/EC, which provides for implementation via sectoral codes of conduct, both on the national and on the European level.

102 Homepage <www.cbweb.nl>.

103 In January 2001, it issued a report on email and Internet privacy in the workplace setting out 17 guidelines for employers.

user information in electronic transactions.¹⁰⁴

According to the Chamber the report “argues in favor of a balanced and common sense approach to e-mail and Internet checks at the workplace.” It concludes that although employees retain a reasonable expectation of privacy in the workplace, employers should be entitled to monitor email and Internet usage under certain conditions.

104

College Bescherming Persoonsgegevens, Annual Report for the Year 2001, July 2002.

8.5.6 In its 2003 annual report the CBP expressed its concern “about the erosion in public debate of the fundamental principle laid down in international treaties that the use of personal data and violation of personal privacy should be an actual necessity”.¹⁰⁵

8.5.7 Two decrees have been issued under the Data Registration Act. The Decree on Sensitive Data¹⁰⁶ sets out the limited circumstances when personal data on an individual’s religious beliefs, race, political persuasion, sexuality, medical, psychological and criminal history may be included in a personal data file. The Decree on Regulated Exemption¹⁰⁷ exempts certain organisations from the registration requirements of the Data Registration Act.

8.5.8 Recent developments include the compulsory identification for all persons from the age of 14 (to have started in 2005) which is intended to increase public safety and the passing, in May 2004, of the law on e-commerce (Wet elektronische handel) that implements the EU E-commerce Directive (2000/31/EC).¹⁰⁸

8.5.9 The Netherlands is a member of the Council of Europe and has signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108).¹⁰⁹ It has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms. In November 2001, the Netherlands signed the Council of Europe Convention on Cybercrime.¹¹⁰ It is a member of the Organisation for Economic Cooperation and Development and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

105 EPIC and Privacy International *Privacy and Human Rights Report 2004* and the references made therein.

106 Decree on Sensitive Data, March 5, 1993.

107 Decree on Regulated Exemption, July 6, 1993.

108 EPIC and Privacy International *Privacy and Human Rights Report 2004* and the references made therein.

109 Signed May 7, 1982; Ratified May 28, 1993; Entered into Force September 1, 1993.

110 Signed November 23, 2001.

8.6 New Zealand¹¹¹

8.6.1 Article 21 of the New Zealand Bill of Rights Act, 1990 states "Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise."¹¹² The New Zealand Court of Appeal has interpreted this provision in several cases as protecting the important values and interests that make up the right to privacy.¹¹³

8.6.2 New Zealand's Privacy Act of 1993 came into force on July 1, 1993. It was preceded by the Privacy Commissioner Act, 1991 which established the office of Privacy Commissioner. It regulates the collection, use and dissemination of personal information across both the public and private sectors. It also grants to individuals the right to have access to personal information held about them by any agency. The Privacy Act applies to "personal information," which means that it is directly concerned with any information about an identifiable individual, whether automatically or manually processed.

8.6.3 The Act contains twelve Information Privacy Principles generally based on the 1980 Organization for Economic and Cooperation Development (OECD) Guidelines and the information privacy principles in Australia's Privacy Act 1988. In addition, the legislation includes a new principle that deals with the assignment and use of unique identifiers. The Information Privacy Principles can be individually or collectively replaced by enforceable codes of practice for particular sectors or classes of information. These codes may modify the application of any of the information

111 EPIC and Privacy International *Privacy and Human Rights Report 2003* at 370 and the references made therein.

112 Bill of Rights Act, 1990, Chapter 4, Section 21, available at <http://www.oefre.unibe.ch/law/icl/nz01000_.html>.

113 Tim McBride, "Recent New Zealand Case Law on Privacy: Part I: Privacy Act and the Bill of Rights Act," *Privacy Law & Reporter*, January 2000, at 107.

protection principles or exempt any action from the principles.¹¹⁴

8.6.4 In addition to the information privacy principles, the legislation contains principles relating to information held on public registers; it sets out guidelines and procedures in respect to information matching programs run by government agencies, and it makes special provision for the sharing of law enforcement information among specialized agencies.

114

See Chapters 4 and 5 above dealing respectively with the privacy principles and codes of conduct.

8.6.5 The Office of the Privacy Commissioner is an independent Crown entity which oversees compliance with the Privacy Act 1993, but does not function as a central data registration or notification authority.¹¹⁵

8.6.6 Complaints by individuals are initially filed with the Privacy Commissioner who attempts to conciliate the matter. The Commissioner regards the power to investigate and to require answers during investigations as "a vital element" in securing such a high conciliation rate. When conciliation fails, the Director of Human Rights Proceedings¹¹⁶ or the complainant (if the Director of Human Rights Proceedings is unwilling) can bring the matter before the Human Rights Review Tribunal, which can issue decisions and award declaratory relief, issue restraining or remedial orders, and award special and general damages up to NZD 200,000. The Privacy Commissioner reports to Parliament through the Minister of Justice under the Public Finance Act.

8.6.7 New Zealand is a member of the Organization for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

8.7 Canada¹¹⁷

115 Homepage <<http://www.privacy.org.nz>.

116 The Director is an official appointed under the Human Rights Act of 1993.

117 EPIC and Privacy International *Privacy and Human Rights Report 2003* at 176 and the references made therein.

8.7.1 There is no explicit right to privacy in Canada's Constitution and Charter of Rights and Freedoms.¹¹⁸ However, in interpreting Section 8 of the Charter, which grants the right to be secure against unreasonable search or seizure, Canada's courts have recognised an individual's right to a reasonable expectation of privacy.¹¹⁹

8.7.2 Privacy is regulated at both the federal and provincial level. At the federal level, privacy is protected by two acts:

- d) the 1982 federal Privacy Act; and
- e) the 2001 Personal Information and Electronic Documents Act (PIPEDA).

8.7.3 The federal Privacy Act of 1982 (which took effect on July 1, 1983) imposes obligations on federal government departments and agencies to respect privacy rights by limiting the collection, use and disclosure of personal information. It provides individuals with a right to access and request correction of personal information about themselves held by those agencies, subject to some exceptions.¹²⁰ Individuals can appeal to a federal court for review if access to their records is denied by an agency, but are not authorised to challenge the collection, use, or disclosure of information.¹²¹ The Act is based on the OECD Guidelines and is thus broadly similar to EU data protection legislation except that it only applies to the public sector.¹²²

118 Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (United Kingdom), 1982, c. 11, s. 8, online: Department of Justice . (date accessed: 25 May 2002).

119 ***Hunter v Southam***, 2 S.C.R. 145, 159-60 (1984).

120 Privacy Act, c. P-21.

121 In 1999, in order to tighten exemptions and loopholes, the Privacy Commissioner finished an extensive review of the Act and recommended over 100 changes to the law to improve and update it. Some of the changes included giving the Commission primary authority over all information collected by the federal government, extending its coverage beyond "recorded" information, increasing notice of disclosures, expanding court reviews, creating rules on data matching, controlling "publicly available" information and expanding the mandate of the Privacy Commissioner. Privacy Commissioner, 1999-2000 Annual Report, May 2000.

122 Privacy and Data Sharing Report fn 2 at 20.

8.7.4 The Personal Information Protection and Electronic Documents Act (PIPEDA) was approved by Parliament in April 2000.¹²³ The Act adopts the CSA International Privacy Code (a national standard: CAN/CSA-Q830-96) into law for private sector organisations that process personal information “in the course of a commercial activity,” and for federally regulated employers with respect to their employees. It does not apply to information collected for personal, journalistic, artistic, literary, or non-commercial purposes.

8.7.5 PIPEDA sets out the ground rules for the collection, use, disclosure, retention, and disposal of personal information. It sets out 10 privacy principles as standards that organisations must comply with when dealing with personal information including: accountability, purpose, openness, consent, limiting use and collection, disclosure, retention, individual access, safeguards, accuracy, and challenging compliance.

123

Bill C-6, Personal Information Protection and Electronic Documents Act.

8.7.6 In January 2001, the Data Protection Working Party of the European Commission issued a decision stating that PIPEDA provided an adequate level of protection for certain personal information transferred from the European Union to Canada.¹²⁴ This will allow certain personal information to flow freely from the European Union to recipients in Canada subject to PIPEDA without additional safeguards being needed to meet the requirements of the European Union Data Protection Directive.

8.7.7 However, the Commission's decision of adequacy does not cover any personal information held by federal sector or provincial bodies or information held by personal organisations and used for non-commercial purposes, such as data handled by charities or collected in the context of an employment relationship.¹²⁵ For this, transfers to recipients in Canada, operators in the European Union will have to put in place additional safeguards, such as the standard contractual clauses adopted by the Commission in June 2001 before exporting the information.

8.7.8 Both the Privacy Act and PIPEDA are overseen by the independent Privacy Commissioner of Canada who is an Agent of Parliament and reports directly to the House of Commons and the Senate. The Commissioner has the power to investigate, mediate, and make recommendations, but cannot issue orders or impose penalties. He or she also conducts periodic audits of federal institutions to determine compliance with the Privacy Act, and to recommend changes where

124 European Union Article 29 Working Party, *Opinion 2/2001 on the Adequacy of the Canadian Personal Information and Electronic Documents Act*, January 26, 2001.

125 Commission Decision of December 20, 2001, Official Journal of the European Communities L 2/13.

necessary.

8.7.9 The Commissioner's powers under PIPEDA are very similar to those under the Privacy Act. Under PIPEDA the Commissioner has investigated:¹²⁶

- a) Air Canada for sharing its customers' personal and financial information with its partners.
- b) a U.S.-based international marketing firm that was disclosing personal information by

126

Examples of investigations under the Privacy Act as referred to in EPIC and Privacy International *Privacy and Human Rights Report 2003* are as follows:

- a) Canadian Customs and Revenue Agency (CCRA) following reports that customs officials were opening mail coming into Canada and passing information relating to immigration cases to Citizenship and Immigration Canada (CIC). [Office of the Privacy Commissioner, New Release , March 19,2001]
- b) Human Resources Development Canada (HRDC) regarding the existence of a government database called the Longitudinal Labour Force File, which could contain up to 2,000 pieces of information on Canadian citizens. The records included tax returns, benefit information, immigration files from the provincial and municipal levels, training information and employment and social insurance master files. The Privacy Commissioner expressed concern about the size of the individual files, their comprehensiveness and the lack of statutory safeguards, the absence of any retention or destruction policy and, above all, the fact that the data base had been compiled largely without the knowledge of Canadian citizens. Publication of the Commissioner's report appears to have resulted in a public outcry, the upshot was an announcement by the HRDC that it was dismantling the longitudinal file and was scrapping the software that allowed sharing with other agencies and returning the information which it had received from them. Privacy and data Sharing Report at 21.[Minister of Human Resources Development Canada, HRDC Dismantles Longitudinal Labour Force File Databank, News Release, May 29, 2000.]
- c) Department of National Defense (DND) for workplace privacy violations, which entailed accessible online employee information.[Privacy Commissioner of Canada Annual Report to Parliament 2000-2001, Part One, n 494.

gathering and selling data on physicians' prescribing patterns.

- c) a Canadian bank's refusal to grant a customer's request for access to their credit score.
- d) a telecommunications company for improperly disclosing a subscriber's unlisted telephone number to a collections agency.

8.7.10 The Bank Act,¹²⁷ Insurance Companies Act,¹²⁸ and Trust and Loan Companies Act¹²⁹ permit regulations regarding the use of information provided by customers. A poll in April 1999 found that 88 percent of people said the government should “not allow banks to use information about their customers' bank accounts and other investments to try to sell customers insurance.”¹³⁰ There are sectoral laws for pensions,¹³¹ video surveillance,¹³² immigration,¹³³ and Social Security.¹³⁴ The Young Offenders Act¹³⁵ regulates the information that can be disclosed about offenders under the age of 18 while the Corrections and Conditional Release Act¹³⁶ speaks to the information that can be disclosed to victims and their families.

8.7.11 In May 2002 Canada became the first national government to make privacy assessments of federal agencies mandatory. The privacy Impact Assessment Policy means that all new and existing

127 Bank Act, c. 46, ss. 242, 244, 459.

128 Insurance Companies Act, s. 489, s. 607.

129 Trust and Loan Companies Act, s. 444.

130 “88% of Canadians Oppose Banks Target-Marketing Insurance: Compass Poll,” *Canada Newswire*, April 27, 1999.

131 Canada Pension Plan, R.S.C. 1985, c. C-8, s. 104.07.

132 Criminal Code, c. C-46, s. 487.01.

133 Immigration Act, S.C. 1985, c. I-2, s. 110.

134 Old Age Security Act, c. O-9, s. 33.01.

135 Young Offenders Act, C. Y-1, s. 38.

136 Corrections and Conditional Release Act, 1992, c. 20, s. 26, 142.

federal programmes with potential privacy risks will undergo a Privacy Impact Assessment (PIA).¹³⁷

8.7.12 Canada is a member of the OECD and relied on the OECD's 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in the drafting of the federal Privacy Act of 1982. Canada also has observer status at the Council of Europe and although it was not a member, it was a key player in the negotiations on the Cybercrime Convention. It has signed, but not yet ratified the Convention.

8.7.13 Privacy legislation on a provincial level is separated into three categories:

- (a) public sector (data protection) law;
- (b) private sector law; and
- (c) sector-specific laws.

137

EPIC and Privacy International *Privacy and Human Rights Report 2004* and the references made therein.

8.7.14 Public sector legislation covering government bodies exists in almost all provinces and territories.¹³⁸ Nearly every province has some sort of oversight body, but they vary in their powers and scope of regulation.

8.7.15 With respect to provincial sector-specific legislation, many provinces have specific laws to protect personal information, including health-specific privacy laws, consumer credit reporting laws, laws regulating information from credit unions, and legislation imposing restrictions on the disclosure of personal information held by private investigators and other professionals.¹³⁹

8.8 Commonwealth of Australia¹⁴⁰

8.8.1 Neither the Australian Federal Constitution¹⁴¹ nor the Constitutions of the six States contain any express provisions relating to privacy. There is periodic debate about the value of a Bill of Rights, but no current proposals. The Constitution limits the legislative power of the Commonwealth (federal) government, with areas not expressly authorised being reserved for the States.

8.8.2 The constitutionality of federal laws imposing privacy rules on the private sector has been questioned, but not challenged so far. Most commentators believe that the Commonwealth could found any private sector privacy law on a 'cocktail' of constitutional powers including those giving

138 A list of state laws and commissions is <<http://infoweb.magi.com/~privcan/other.html>>.

139 Alberta, Manitoba, and Saskatchewan have all passed health-specific privacy legislation, which sets rules for the collection, use, and disclosure of personal health information. These laws apply to personal health information held by hospitals, government ministries, regulated health professionals, and other health care facilities. Ontario is currently working on including health privacy legislation in its general private sector legislation. Sectoral laws, however, only provide a partial and fragmentary approach to the problem of regulation. Privacy Commissioner **Report to Parliament on Substantially Similar Provincial Legislation**, May 2002.

140 EPIC and Privacy International **Privacy and Human Rights Report 2003** at 139 and the references made therein.

141 The Commonwealth of Australia Constitution Act.

authority over telecommunications, corporations and foreign affairs (e.g. treaties).

8.8.3 Privacy Law in Australia comprises a number of Commonwealth (federal) statutes covering particular sectors and activities,¹⁴² some State or Territory laws with limited effect, and the residual common law protections, which have very occasionally been used in support of privacy rights through actions for breach of confidence, defamation, trespass or nuisance.

8.8.4 The principal federal statute is the Privacy Act of 1988¹⁴³ which has four main areas of application, and which gives partial effect to Australia's commitment to the OECD Guidelines and to the International Covenant on Civil and Political Rights (ICCPR).

8.8.5 The Privacy Act provides for:

- f) eleven Information Privacy Principles (IPPs), based on those in the OECD Guidelines that apply to the activities of most federal government agencies.
- g) a separate set of rules about the handling of consumer credit information, added to the law in 1989, that applies to all private and public sector organisations.
- h) the monitoring of the processing of the government issued Tax File Number (TFN), by organisations authorised to record such information (the entire community is subject to Guidelines issued by the Privacy Commissioner which take effect as subordinate legislation).

8.8.6 The origins of the Privacy Act were the protests in the mid-1980s against the Australia Card scheme – a proposal for a universal national identity card and number. This proposal was dropped, but use of the tax file number was enhanced to match income from different sources with the Privacy Act providing some safeguards. The use of the tax file number has been further extended by law to

142 Such as the Telecommunications Act 1979 (Cth) which regulates the interception of telecommunications and the Crimes Act 1914 (Cth) which contains a variety of privacy-related measures including offences relating to unauthorised access to computers, interception of mail and telecommunications and the disclosure of Commonwealth government information

143 Privacy Act 1988 (Cth).

include benefits administration as well as taxation. Some controls over this matching activity were introduced in 1990.¹⁴⁴

8.8.7 The Privacy Act was extended by the Privacy Amendment (Private Sector) Act 2000(Commonwealth) to cover private sector organisations, passed in December 2000 and which took effect in December 2001.

144 The Data-matching program (Assistance and Tax) Act 1990.

8.8.8 The law provides for ten National Privacy Principles (NPPs) based on the National Principles for Fair Handling of Personal Information originally developed by the Federal Privacy Commissioner in 1998 as a self-regulatory substitute for legislation. It applies to parts of the private sector and all the health service providers. Private companies are now required to observe these principles although they can apply to the Privacy Commissioner for approval of a self-developed Code of Practice containing principles that are an “overall equivalent” to the NPPs. The Act has been criticised as failing to meet international standards of privacy protection.¹⁴⁵

8.8.9 It has been argued that the NPPs impose a lower standard of protection in several areas than the European Union Directive. For example:

- a) organisations are required to obtain consent from customers for secondary use of their personal information for marketing purposes where it is “practicable”; otherwise, they can initiate direct marketing contact, providing they give the individual the choice to opt out of further communications;
- b) controls on the transfer of personal information overseas are also limited, requiring only that organisations take “reasonable steps” to ensure personal information will be protected, or “reasonably believes” that the information will be subject to similar protection as applied under Australian law;
- c) in addition, the Act provides for a number of broad exemptions for employee records (defined as a record of personal information relating to the employment of the employee including, for example, health information, contact details, salary or wages, performance and conduct, trade union membership, recreation and sick leaves, banking affairs etc); media organisations (defined to include organisations which provide information to the public and political parties); and small businesses (defined as receiving under \$A3m annual turnover and not disclosing personal information for a benefit);¹⁴⁶

145

See Roger Clarke’s Homepage <<http://www.anu.edu.au/people/Roger.Clarke/>>.

146

According to the Federal Government the small business exemption exempts about 94 percent of all Australian businesses but only 30 percent of total business sales. Gunning P “Central Features of Australia’s Private Sector

- d) there are also weaknesses in the enforcement regime including, for example, allowing privacy complaints to be handled by an industry-appointed code authority with limited oversight by the Privacy Commissioner.

8.8.10 The Act does, however, include an innovative principle of anonymity. Principle 8 states that: “Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering into transactions with an organisation.”

8.8.11 The Article 29 Data Protecting Working Party of the European Commission expressed many reservations about the Act in its report (dated March 2001), suggesting that it would not, as currently written, satisfy the adequacy test in Articles 25 and 26 of the European Union directive for data to flow to third countries.¹⁴⁷ The group recommended the introduction of additional safeguards to address these concerns.

8.8.12 In response, the Attorney General issued a press release stating that the Committee's comments "display an ignorance about Australia's law and practice and do not go to the substance of whether our law is fundamentally "adequate" from a trading point of view." He acknowledged that officials from Australia and Europe would "obviously" continue to talk but that "Australia will only look at options that do not impose unnecessary burdens on business."¹⁴⁸ In April 2004 the Privacy Commissioner urged a move away from the initial strategy of cooperation with the business sector towards greater enforcement. The Privacy Amendment Act of 2004 furthermore extended data - correction rights to non-Australian citizens.¹⁴⁹

147 European Union Article 29 Working Party *Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000.*

148 The AG's Department has, however, begun a joint review with the Department of Employment, Workplace Relations and Small Business to examine State, Territory and Commonwealth workplace relations legislation and the privacy protection of employee records. The time line for this review is unclear, although it is expected to be completed within two years of the commencement of the legislation. The Department is also looking into the need for specific privacy protection for children's personal information.

149 EPIC and Privacy International *Privacy and Human Rights Report 2004* and the references made therein.

8.8.13 The Office of Privacy Commissioner,¹⁵⁰ which has responsibilities under the Privacy Act, was initially established as a member of the Human Rights and Equal Opportunity Commission but has been operating as a separate statutory agency since 1st July 2000.

150

Homepage <<http://www.privacy.gov.au/>>.

8.8.14 The Office has a wide range of functions, including handling complaints, auditing compliance, promoting community awareness, and advising the government and others on privacy matters. The Commissioner's office, which was cut back in the late 90's, recently received additional resources in anticipation of the new private sector jurisdiction.¹⁵¹

8.8.15 The federal Privacy Commissioner is also the supervisory and complaint handling agency of Part VIIC of the Crimes Act enacted in 1989¹⁵² and the Data-matching Program (Assistance and Tax) Act 1990.¹⁵³

8.8.16 On July 31, 2001 the Privacy Commissioner released the results of a comprehensive research project into public attitudes towards privacy issues that was commissioned earlier in the year.¹⁵⁴

The research findings were incorporated into three separate reports:

- a) Privacy and the Community;

151

Work done by the Commission:

- a) In September 2001, the Privacy Commissioner issued the finalised Guidelines on the implementation of the NPPs and a revised draft of the Guidelines on the development of industry codes.
- b) **In April 2002, the Privacy Commissioner approved the first private sector code, submitted by the Insurance Council of Australia (ICA).** Office of the Federal Privacy Commissioner, Media Release, "Federal Privacy Commissioner Approves Australia's First Privacy Act Privacy Code," April 17, 2002, Under the new General Insurance Information Privacy Code, complaints concerning the general insurance industry will be handled by the Privacy Compliance Committee, a committee of the Insurance Enquiries and Complaints Ltd, rather than the Privacy Commissioner. The Internet Industry Association is also drafting a code that it hopes will meet the European Union requirements. Karen Dearne, Privacy Safety Net for European Union, Australia IT News, December 11, 2001. Other industries that have already adopted self-regulatory initiatives (e.g. the direct marketing and telecommunications industries) will have to decide whether to apply to register their Codes of Practice, and their alternative dispute resolution schemes, under the Privacy Act.
- c) **In March 2002 the Commissioner signed an agreement with the Australian Competition and Consumer Commission, which enforces existing fair trading rules, to facilitate cooperation and coordination between the offices where standards overlap.** Office of the Federal Privacy Commission, "Regulators Co-Operate to Improve Privacy Compliance," Media Release, 12 March 2002.

152

Which provides some protection to individuals who have had criminal convictions in relation to so-called 'spent' convictions (i.e.: convictions for relatively minor offences which they are allowed to 'deny' or have discounted after a set period of time).

153

That provides detailed procedural controls over the operation of a major program of information matching between federal tax and benefit agencies.

154

Office of the Federal Privacy Commissioner of Australia ***The Results of Research into Community, Business and Government Attitudes Towards Privacy in Australia*** July 31 2001.

- b) Privacy and Business; and
- c) Privacy and Government.

8.8.17 The results showed overwhelming support for privacy protection.¹⁵⁵ The Privacy Commissioner indicated that the results of the survey would be used in the future planning of the office.

8.8.18 Some Australian States and Territories also enacted separate privacy laws.

155

For example, 91 percent of the public said that they would like businesses to seek permission before engaging in direct marketing; 89 percent would like organisations to advise them who would have access to their personal information and 92 percent would like to be told how it would be used; 42 percent have refused to deal with organisations they felt did not adequately protect their privacy. When asked what kind of data they considered most sensitive 40 percent identified financial details, 11 percent identified income, 7 percent identified medical or health information, 4 percent identified home address, 3 percent identified phone number and 3 percent identified genetic information. Office of the Federal Privacy Commissioner *Privacy and the Community: Main Findings*.