

Chapter 13

Technology

- 13.1 In this chapter we outline some key technological developments and consider the Privacy Act issues that they may give rise to. The range of topics covered is necessarily selective, and it is by no means a comprehensive survey.¹⁰⁵² The pace of change in this area means that new technological issues are constantly arising. We have selected topics that affect large numbers of New Zealanders or give rise to important privacy issues. At the end of the chapter we ask for views as to whether there are any other technology issues that submitters believe warrant particular consideration. We are not technology experts, and we invite comments and submissions from those who are. We also welcome the views of anyone with an interest in these topics.
- 13.2 We have endeavoured to ensure that the material in this chapter is up-to-date at the time of writing. Due to the rapid pace of change, however, some of the statements made, and material referred to in this paper, may quickly become outdated.

BACKGROUND

- 13.3 Technological advances have made it technically and economically feasible to collect, use, store and re-use massive amounts of personal information in a variety of contexts for multiple purposes. These developments have been embraced in both the public and private sectors, where there is significant reliance on the collection, use, sharing and repackaging of personal data. Consequently, personal data has become increasingly commoditised.¹⁰⁵³
- The provision of public services of all kinds has become dependent on data collection, sharing, and other related practices. Government activity is dependent on the use of personal data. The economy is fuelled by information processing. Many companies build their businesses around the collection and analysis of data.
- 13.4 The information practices which these technological developments give rise to are on a new scale from traditional paper records or early computer databases. The Office of the Privacy Commissioner's current Statement of Intent notes that rapidly changing technologies, internet fraud and safety, cloud computing and

1052 See also Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) chapter 9.

1053 House of Lords Constitution Committee *Surveillance: Citizens and the State* (London, 2009) para 47.

cross-border data processing all raise challenging information and privacy issues.¹⁰⁵⁴ The impacts of the internet and social networking on privacy, in particular young people's privacy, are increasingly important.¹⁰⁵⁵

Opinion surveys indicate that New Zealanders are concerned about the misuse of personal information and invasion of individual privacy by technology. Unease exists around privacy intrusions in areas such as social networking, the internet, employment, finance, telecommunications and health.

- 13.5 The digital revolution continues to create a wealth of personal data about people and their activities. Some might ask whether there is any realistic prospect that personal privacy can be protected in the new digital era, and whether it is worth attempting to protect digital privacy, given the economic benefits to the private sector and the increased efficiency to the public sector that technological developments relating to data have given rise to.
- 13.6 Nevertheless, while technological transformations undoubtedly bring great benefits and efficiencies, they also create potentially significant societal and individual costs,¹⁰⁵⁶ such as loss of control over the collection and use of personal information, the potential for increased surveillance and an associated chilling effect on citizens, reduced trust in relationships between citizens and business or government with consequential reduced participation, and an increased risk of detrimental consequences including identity crime.¹⁰⁵⁷ There are also commercial benefits to privacy protection (whether online or offline) including customer retention, reduced reputational risk and efficiency gains. We therefore see data protection as continuing to have an important role in the digital context.
- 13.7 In fact, the role of data protection may become even more crucial in light of technological developments. As people engage more completely with digital technologies, the amount of digital data proliferates, as do the number of spin-off profiles that begin to accrue.¹⁰⁵⁸

[T]he danger is that what is relevant is no longer personhood – the recognition of a person as having status as a person – but rather a profile – the recognition of a pattern of past behaviour. ... The ability to control the use of one's identity information is crucial for reminding others that there is a person behind data and enabling that person to have full status when dealing with others.

1054 Office of the Privacy Commissioner *Statement of Intent 2009/10 – 2012/2013* (Wellington, 2009) 3.

1055 Office of the Privacy Commissioner *Statement of Intent 2009/10 – 2012/2013* (Wellington, 2009) 10.

1056 See discussion of Solove's harm-based analysis in New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) paras 3.26–3.32.

1057 See discussion of informational privacy risks in New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) paras 3.40–3.49.

1058 OECD Directorate for Science, Technology and Industry *At a Crossroads: "Personhood" and Digital Identity in the Information Society* (Paris, 2007) 10.

13.8 In *Privacy: Concepts and Issues*, we outlined some of the key technological developments that potentially impact on privacy, including:¹⁰⁵⁹

- developments relating to computers and digital data, such as advances in computer technology and data collection and analysis;
- developments relating to the internet, such as the collection of personal information online, the availability of personal information and images online and targeted advertising;
- surveillance and location technologies such as visual surveillance and radio frequency identification; and
- technologies of the body, such as biometric and genetic technologies and brain scanning.

We also noted that privacy-enhancing technologies have a role in ensuring that developing technologies offer privacy safeguards.¹⁰⁶⁰

FUNCTIONS OF THE PRIVACY COMMISSIONER

13.9 Certain functions of the Privacy Commissioner specifically relate to technological developments. These empower him or her to:¹⁰⁶¹

- inquire generally into any matter, including any enactment or law, or any practice, or procedure, whether governmental or non-governmental, or *any technical development*, if it appears to the Commissioner that the privacy of the individual is being, or may be, infringed thereby;¹⁰⁶² and
- undertake research into, and to monitor developments in, *data processing and computer technology* to ensure that any adverse effects of such developments on the privacy of individuals are minimised, and to report to the responsible Minister the results of such research and monitoring.¹⁰⁶³

13.10 Other generic functions of the Privacy Commissioner are also relevant, such as undertaking educational programmes;¹⁰⁶⁴ making public statements in relation to any matter affecting the privacy of the individual;¹⁰⁶⁵ consulting and co-operating with other bodies;¹⁰⁶⁶ recommending to the Prime Minister legislative or other action;¹⁰⁶⁷ and recommending to the Prime Minister the acceptance of any international instrument relating to privacy.¹⁰⁶⁸

1059 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) chapter 6.

1060 New Zealand Law Commission *Privacy: Concepts and Issues*, (NZLC SP19, Wellington, 2008) paras 6.103–6.120.

1061 The functions of the Privacy Commissioner are also discussed in chapter 6.

1062 Privacy Act 1993, s 13(1)(m).

1063 Privacy Act 1993, s 13(1)(n).

1064 Privacy Act 1993, s 13(1)(g).

1065 Privacy Act 1993, s 13(1)(h).

1066 Privacy Act 1993, s 13(1)(j).

1067 Privacy Act 1993, s 13(1)(p).

1068 Privacy Act 1993, s 13(1)(q).

- 13.11 The development of new technologies is identified by the Privacy Commissioner to be an important driver for the office's activities: "Monitoring and advising upon technology developments will remain a major priority, given the strong and widespread impact on individual privacy through these changes."¹⁰⁶⁹
- 13.12 Through various forums and networks, the Office of the Privacy Commissioner (OPC) monitors new technologies and reviews their impacts on the protection of personal information.¹⁰⁷⁰ The Privacy Commissioner also participates in international privacy fora such as the International Working Group on Data Protection and Telecommunications (also known as "the Berlin Group") and the OECD Working Party on Information Security and Privacy (WPISP).
- 13.13 The Privacy Commissioner's website devotes a section to "You, your privacy and technology", with tips for online privacy, such as privacy pointers for subscribing to online services, shopping online and online banking.¹⁰⁷¹ There are also links provided on topics such as government use of biometric technologies; "smart" transport payment systems; social networking online; public attitudes to CCTV camera surveillance; and sensors in everyday life.
- 13.14 One of the Privacy Commissioner's operating intentions is to assist with achieving improved privacy standards and practice in government and business. A long term impact sought by the OPC is the harnessing of the benefits of technology by New Zealand businesses while better understanding privacy risks and solutions.¹⁰⁷² Key activities planned include:¹⁰⁷³
- monitoring and advising on the privacy impacts of proposed legislation, policy and technology initiatives;
 - continuing to contribute to and help guide e-government initiatives; and
 - publishing additional resources, particularly web-based publications and case notes, including those focusing on technology, privacy and business needs.
- 13.15 Recent work by the OPC on privacy issues associated with technological developments includes the release of guidance on the use of CCTV cameras,¹⁰⁷⁴ and a guidance note on the use of portable storage devices in business and government.¹⁰⁷⁵ The Privacy Commissioner has also produced information about layered privacy notices (including privacy notices for websites)¹⁰⁷⁶ and a *Privacy Impact Assessment Handbook* (with comments and suggestions particularly suited to projects with a technological component).¹⁰⁷⁷

1069 Office of the Privacy Commissioner *Statement of Intent 2009/10 – 2012/2013* (Wellington, 2009) 9.

1070 Office of the Privacy Commissioner *Statement of Intent 2009/10 – 2012/2013* (Wellington, 2009) 17. The Privacy Commissioner intends to hold four Technology and Policy Forums in the next operating period.

1071 Office of the Privacy Commissioner www.privacy.org.nz/you-your-privacy-and-technology (accessed 11 December 2009).

1072 Office of the Privacy Commissioner *Statement of Intent 2009/10 – 2012/2013* (Wellington, 2009) 12.

1073 Office of the Privacy Commissioner *Statement of Intent 2009/10 – 2012/2013* (Wellington, 2009) 13.

1074 Office of the Privacy Commissioner *Privacy and CCTV: a Guide to the Privacy Act for Businesses, Agencies and Organisations* (Wellington, 2009).

1075 Office of the Privacy Commissioner *Guidance Note on the use of Portable Storage Devices* (Wellington, 2009).

1076 Office of the Privacy Commissioner *Questions and Answers about Layered Privacy Notices* www.privacy.org.nz (accessed 15 January 2010).

1077 Office of the Privacy Commissioner *Privacy Impact Assessment Handbook* (Wellington, 2007).

- 13.16 The Privacy Act 1988 (Cth) provides for the establishment of a Privacy Advisory Committee, convened by the Australian Privacy Commissioner and made up of government and industry representatives. One member is to have extensive experience in “electronic data processing”, which the Australian Law Reform Commission (ALRC) has recommended be changed to experience in “information and communication technologies.”¹⁰⁷⁸ The ALRC has also recommended that the Australian Privacy Commissioner have an express legislative power to establish expert panels as a tool to deal with difficult and emerging areas of privacy regulation, including new and developing technologies.¹⁰⁷⁹
- 13.17 The ALRC has also recommended that the Australian Privacy Commissioner should develop and publish guidance in relation to technologies that impact on privacy,¹⁰⁸⁰ such guidance to address certain matters including:
- developing technologies such as radio frequency identification (RFID) or data-collecting software such as “cookies”;
 - when the use of a certain technology to collect personal information is not done by “fair means” and is done in an “unreasonably intrusive way”;
 - when the use of a certain technology will require agencies and organisations to notify individuals at or before the time of collection of personal information; and
 - when agencies and organisations should notify individuals of certain features of a technology used to collect information (for example, how to remove an RFID tag contained in clothing; or error rates of biometric systems).

Q155 Do you have any comments on the role and functions of the Privacy Commissioner in relation to technological developments? Should the Privacy Commissioner’s functions in relation to technology be revised and should any new functions be added?

Q156 Should the Privacy Act provide for a Privacy Advisory Panel, or empower the Privacy Commissioner to set up expert panels on particular issues, as the Australian Privacy Act does?

1078 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) paras 46.72–46.100, recommendation 46-4(c).

1079 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) paras 46.101–46.108, recommendation 46-5.

1080 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) recommendation 10-3. See also the recommendations of the Australian Law Reform Commission in relation to biometrics and Privacy Impact Assessments, outlined below.

THE IMPACT OF TECHNOLOGY ON THE PRIVACY ACT FRAMEWORK

- 13.18 New technological developments create pressure points on the existing Privacy Act framework in a number of key ways. Greater uptake of technological applications has reduced de facto privacy protections such as information being widely dispersed and difficult to access, and limitations on physical storage.¹⁰⁸¹ Rapid technological change places increased pressures on personal information handling practices and quickly outstrips conventional information handling techniques.¹⁰⁸²
- 13.19 Key privacy principle concepts such as notice and consent may not always be effective in the online environment. Notice in the form of privacy policies is not always user-friendly or sufficiently transparent, and can be easy for users to ignore. Consumers do not always know what they are consenting to, especially regarding secondary uses of their data, and who their data will be shared with.¹⁰⁸³
- 13.20 Technology can facilitate vast collections and disclosures of personal information that may affect a large number of people, even though the effects on individuals may be small. Online data collection and use can affect an individual's ability to control his or her personal information without necessarily resulting in demonstrable "harm". While there may sometimes be little measurable harm caused in individual terms, the impact in terms of the societal value of privacy and public confidence may be significant. The Privacy Act's complaints process can only be used if there has been "harm" to the individual concerned,¹⁰⁸⁴ however, some of the Privacy Commissioner's other functions extend to addressing systemic issues.

Cross-border issues

- 13.21 Technological changes and the internet pose new challenges for the regulation of agencies that collect, hold or use the personal information of New Zealanders but do not have any physical presence in New Zealand. While "New Zealanders want their personal information protected wherever it travels",¹⁰⁸⁵ it may be difficult to enforce the New Zealand privacy principles against offshore entities. Issues associated with trans-border data flows are discussed in chapter 14.

Technological neutrality

- 13.22 The privacy principles are technologically neutral in that they apply to "information", regardless of the form in which it is held.¹⁰⁸⁶ Thus the legislation is capable of applying to new technologies that enable the collection, use and disclosure of personal information. The Privacy Commissioner has suggested

1081 Senator John Faulkner "Privacy – where do you draw the line?" (Speech to Australian Public Service Commission, Canberra, 8 May 2009).

1082 Office of the Privacy Commissioner *Statement of Intent 2009/10 – 2012/2013* (Wellington, 2009) 9.

1083 Wendy Davis "Web Privacy Practices Fall Short" (4 June 2009) *Online Media Daily* www.mediapost.com (accessed 26 June 2009).

1084 Privacy Act 1993, s 66. In chapter 8 we propose that the harm threshold for complaints should be removed.

1085 Office of the Privacy Commissioner *Statement of Intent 2009/10 – 2012/2013* (Wellington, 2009) 14.

1086 Gehan Gunasekara "'MySpace' or Public Space: the Relevance of Data Protection Laws to Online Social Networking" (2008) 23 NZULR 191, 198.

that the rate of technological change favours retaining technologically neutral principles, to reduce the need for constant updating of legislation in the face of new developments.¹⁰⁸⁷

- 13.23 Nevertheless, the adequacy of existing data protection safeguards as applied to the emerging information society is being questioned.¹⁰⁸⁸ It has been suggested that privacy rights in the online environment are diluted, inadequately protected and difficult to enforce.¹⁰⁸⁹ The privacy principles are based on OECD guidelines developed in the 1970s. At that time, when the internet was in a state of relative infancy, the key privacy concerns related to issues associated with databases.¹⁰⁹⁰ The rapid rate of technological change since then raises the question of whether the concept of technological neutrality, as embedded in the privacy principles, remains effective, or whether it has been somewhat eclipsed, given the variety of ways in which information about individuals and their activities can now be collected, aggregated, stored, used and re-used.
- 13.24 The ALRC has concluded that it would be undesirable to recommend significant changes to the Australian Privacy Act's privacy principles to accommodate technologies which are yet to be invented or deployed, and that, where possible, provisions of the Privacy Act should be technology neutral.¹⁰⁹¹ However, the ALRC did not foreclose the possibility of technology-specific regulation in certain circumstances, such as through codes of practice.¹⁰⁹²

The global context

- 13.25 Because of the cross-border nature of the internet and the information handling practices that it gives rise to, we do not see that it is practical to try to formulate significant reforms to New Zealand's Privacy Act framework in isolation from international responses and regulatory practices. New Zealand is a relatively small participant in the international marketplace and its influence on global practices is limited. It would make little sense for New Zealand to strike out and establish a particular approach to technology-related privacy issues that is out of step or incompatible with the approaches of more influential jurisdictions, or approaches endorsed by regional or co-operative blocs such as the EU, APEC and the OECD.¹⁰⁹³ While it remains important for New Zealand to maintain a robust privacy framework to regulate domestic privacy issues related to technological developments, reform also needs to be mindful of the international context.¹⁰⁹⁴

1087 *Necessary and Desirable* 17.

1088 OECD Directorate for Science, Technology and Industry *At a Crossroads: "Personhood" and Digital Identity in the Information Society* (Paris, 2007) 6.

1089 Office of the Privacy Commissioner (Cth) *Getting in on the Act: the Review of the Private Sector Provisions of the Privacy Act 1988* (Sydney, 2005) para 8.2, citing submission of Electronic Frontiers Australia.

1090 *Necessary and Desirable* 15–16.

1091 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) para 10.9.

1092 See for example the Biometrics Institute Privacy Code approved by the Australian Privacy Commissioner.

1093 See *Necessary and Desirable* 17. See discussion of the approaches of the EU, APEC and the OECD in chapter 14.

1094 See chapter 14.

- 13.26 New Zealand policy can be informed by international efforts to address technology-related privacy issues. International organisations and privacy regulators devote significant effort and resources to debating and proposing reforms. New Zealand citizens also benefit indirectly from the actions of overseas privacy regulators. Where challenges to practices result in improved privacy standards, this may benefit the global community, not just users in the privacy regulator's home jurisdiction.¹⁰⁹⁵

Q157 Is the basic framework of the Privacy Act adequate to deal with technological change? Should the privacy principles remain technologically neutral?

THE INTERNET AND THE PARTICIPATORY WEB 2.0

- 13.27 In this section we outline issues arising through the use of search engines, websites and social networking sites such as Facebook, MySpace, and Bebo. The internet and the possibilities it has brought with it pose challenges for the privacy of individuals. The World Wide Web is constantly adapting and its limits continue to expand. Websites are now more accessible and allow for an increasingly inter-active experience. New Web 2.0 sites give users greater control over the content of pages, allowing them to upload their own information, add to pre-existing information, and interact with the information of others. These sites include blogs, social networking sites and other sites such as Flickr and YouTube that allow users to upload their photos and videos for others to access.
- 13.28 In *Privacy: Concepts and Issues*, we observed that New Zealanders are enthusiastic users of the internet.¹⁰⁹⁶ The authors of *The Internet in New Zealand* found that 78 per cent of New Zealanders use the internet.¹⁰⁹⁷ The same study showed that New Zealanders spend a large number of hours on the internet for personal, non-work-related purposes.¹⁰⁹⁸ Other research has shown that our common internet activities include general Web surfing or browsing, internet banking, searching for information on goods and services, and listening to music.¹⁰⁹⁹

1095 For example, see the Canadian Privacy Commissioner's investigation into Facebook, discussed below.

1096 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008), para 6.22.

1097 A Bell and others *The Internet in New Zealand 2007: Final Report* (Institute of Culture, Discourse and Communication, AUT University, Auckland, 2008) 3. Of the 22 per cent that are not users, six per cent are ex-users, and only sixteen per cent have never used the internet.

1098 A Bell and others *The Internet in New Zealand 2007: Final Report* (Institute of Culture, Discourse and Communication, AUT University, Auckland, 2008) 3.

1099 Margie Comrie, Franco Vaccarino, Susan Fountaine and Bronwyn Watson *Media Literacy Information in New Zealand: A Comparative Assessment of Current Data in Relation to Adults* (Broadcasting Standards Authority, Wellington, 2007) 41–51.

- 13.29 OPC’s website offers internet users guidance about their personal privacy and the internet with information about how personal information is collected by websites and search engines, and what users can do to prevent or mitigate any privacy harms that may arise through the use of the internet.¹¹⁰⁰ The website notes that the Privacy Act does not generally apply to non-New Zealand agencies. This highlights the Privacy Commissioner’s limited jurisdiction to act in relation to data handling practices that occur outside New Zealand.
- 13.30 Personal information handling in an online environment can give rise to various Privacy Act issues including:
- whether online information is “personal information” for the purposes of the Privacy Act;¹¹⁰¹
 - whether the information is “publicly available information” within the exception to the collection, use and disclosure principles;
 - whether privacy policies are adequate so that acceptance can be considered to constitute consent to data handling practices for purposes of the privacy principles;¹¹⁰²
 - whether the access and correction principles apply or whether the data collection is outside the scope of the Privacy Act; and
 - whether the Privacy Act complaints process is available or whether any interference with privacy occurred outside New Zealand and is therefore outside the scope of the Privacy Commissioner’s authority to act.¹¹⁰³
- 13.31 One issue fundamental to the interface between users and the online environment is identity management. The Information and Privacy Commissioner of Ontario has issued a report on this topic, suggesting that debate is needed about the development of mechanisms to assure the security and privacy of identity information:¹¹⁰⁴

Almost all online activities, such as sending emails, filing tax declarations, managing bank accounts, buying goods, playing games, connecting to a company intranet, and meeting people in a virtual world, require identity information to be given from one party to another. Today, most users have to establish their identity each time they use a new application, usually by filling out an online form and providing sensitive personal information (e.g. name, address, credit card number, phone number etc.).

A typical Internet user in Canada has provided some type of personal information to dozens of different websites. If you count cookies and IP addresses as personal information, then Internet users have left behind personally identifiable information everywhere they’ve been. They have left “digital bread crumbs” throughout cyberspace – and they have little idea how that data might be used or how well it is protected.

1100 See Office of the Privacy Commissioner “You, Your Privacy and Technology” www.privacy.org.nz/you-your-privacy-and-technology (accessed 11 December 2009).

1101 This may be problematic where individual pieces of information can be brought together from various internet sources which in aggregated form may comprise of personal information.

1102 See Alan Toy “Consent to Online Privacy Policies” (2009) 15 NZBLQ 235.

1103 See chapter 14 on cross border issues.

1104 Ann Cavoukian, Information and Privacy Commissioner of Ontario *Privacy in the Clouds, A White Paper on Privacy and Digital Identity: Implications for the Internet* (Toronto, 2008) 9.

The report suggests that what is needed is flexible and user-centric identity management, so that through informed consent, individuals have better control over their personal information that is used for identity authentication purposes, as well as reducing the risk of identity fraud and the potential for online surveillance and profiling.

Search engines and websites

- 13.32 As we outlined in *Privacy: Concepts and Issues*, there is an abundance of information that can be collected about individuals from their online activities such as using search engines and visiting websites.¹¹⁰⁵ Data is provided by internet users both consciously (for example, registering on websites) and unconsciously (for example, search terms and click stream data). The incentive to collect online data derives from its usefulness both for website design, customisation and maintenance, and for the purpose of online targeted advertising.¹¹⁰⁶ In the public sector, internet data is collated for understanding and optimising web usage.¹¹⁰⁷
- 13.33 Through technical means such as the use of cookies,¹¹⁰⁸ search engines collect the terms typed into a search engine by an individual user, the IP address of the user's computer, "click stream data", and a unique identifier for the user's web browser.¹¹⁰⁹ Search engines can also collect the personal information of users required to sign in to be able to use particular services, such as email.¹¹¹⁰
- 13.34 Click stream data is collected by search engines in the form of search histories, as well as by web site operators and third party advertisers and trackers through the placement of tracking cookies on the user's machine and the use of web bugs,¹¹¹¹ a process which is largely invisible to users. In the private sector, collected data may then be shared with affiliate entities, or sold and purchased between site operators to enhance profiles.¹¹¹²
- 13.35 Search engines also enable users to pull together information about an individual from all over the internet, creating a full and sensitive picture of that individual. In this regard it has been noted that: "The personal information a user posts online, combined with data outlining the user's actions and interactions with

1105 New Zealand Law Commission *Privacy: Concepts and Issues*, (NZLC SP19, Wellington, 2008) paras 6.24–6.30.

1106 Targeted advertising is discussed in more detail in chapter 15.

1107 Center for Democracy & Technology and Electronic Frontier Foundation *Open Recommendations for the Use of Web Measurement Tools on Federal Government Web Sites* (Washington, DC, 2009) 1.

1108 "Cookies" are small pieces of code that some web sites place in the computer hard drive of users who visit the website. Cookies collect header information about the visitor and may include click stream data and may also record any information that a user is requested to supply to a website: New Zealand Law Commission *Electronic Commerce Part Three – Remaining Issues* (NZLC R68, Wellington, 2000) 25.

1109 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) para 6.26.

1110 Two common examples include Google and Yahoo which offer both email and search services.

1111 For discussion of web bugs see UC Berkeley, School of Information *Know Privacy* (Berkeley (CA), 2009) 8. The study concluded that web bugs are ubiquitous on the web.

1112 For example, Google has five web trackers: Analytics, DoubleClick, AdSense, FriendConnect, and Widgets.

other people, can create a rich profile of that person's interests and activities."¹¹¹³ The ability to access so much information about people may increase their chances of becoming victims of identity theft or fraud.¹¹¹⁴

Privacy issues

13.36 The internet has undoubtedly brought huge benefits to business, government and the individual citizen. But it also poses numerous privacy challenges for individuals. Search engines and websites collect and monitor the personal information of users, often when the user is unaware that this is occurring. This information can be retained indefinitely, with limited or no benefit for the user. Although much of it is anonymised, information may be tracked back to an individual user through his or her IP address.¹¹¹⁵ Consent to collect personal information is not always sought in a transparent way.

13.37 One view is that the online collection of personal data is simply the corollary of the collection of offline data: "At least when I am online I assume that I am being tracked, and frankly, I don't care."¹¹¹⁶ But when asked about online privacy, most people say they want more information about how they are being tracked and more control over how their personal information is used.¹¹¹⁷ In a 2008 survey commissioned by the OPC, 82 per cent of respondents were concerned (including 62 per cent very concerned) about the "security of personal information on the internet" and two-thirds said they were uncomfortable about internet search engines and social networking sites tracking internet use and emails in order to deliver targeted advertising.¹¹¹⁸ According to one study:¹¹¹⁹

There is overwhelming evidence from various surveys to show that users are concerned about the collection of data by websites. These surveys also show that users desire control of who can collect or see data about them and for what purposes. However, despite these concerns and desires, the studies also show that users are often ignorant of how data collection works, whether it is within the scope of the law and how to stop it.

13.38 Some of the information that is collected by search engines and websites is capable of being used to identify an individual person. IP addresses are the primary means by which information submitted to web sites and search engines

1113 Article 29 Data Protection Working Party *Opinion 5/2009 on Online Social Networking* (12 June 2009) 01189/09/EN WP163, 4.

1114 Identity theft is discussed in chapter 17.

1115 For discussion of the limits of anonymisation to protect informational privacy, see Paul Ohm "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (University of Colorado Law Legal Studies Research Paper No 09-12, 2009).

1116 George Simpson "I'm Being Followed and I Don't Care" (25 June 2009) *Online Media Daily* www.mediapost.com (accessed 26 June 2009). See also Wendy Davis "How Much Targeting is Too Much?" (24 June 2009) *Online Media Daily* www.mediapost.com (accessed 26 June 2009).

1117 Miguel Helft "Google is Top Tracker of Surfers in Study" (2 June 2009) <http://bits.blogs.nytimes.com> (accessed 24 February 2010).

1118 Office of the Privacy Commissioner *Individual Privacy and Personal Information Survey 2008* www.privacy.org.nz (accessed 13 January 2010).

1119 UC Berkeley, School of Information *Know Privacy* (Berkeley (CA), 2009) 17.

becomes personally identifiable.¹¹²⁰ This information can also be tracked back to individual users or computers through analysing the search terms individuals enter into computers (including “vanity” searches which involve individuals using search engines to seek out information about themselves held on the internet), and through the use of cookies. Some cookies are beneficial to users; for example, they may configure a news page in a manner that a user has requested during a previous visit. But they also carry privacy concerns for individuals. Users are rarely aware that cookies are being placed on their hard drives by any particular website, limiting the ability to give informed consent to the collection practices of a particular site.

- 13.39 Of primary concern is the lack of transparency around the collection, retention and use of the personal information. Most users are unaware that search engines and websites are collecting their personal information and the purposes this information is being collected for. Users are therefore unable to give informed consent to the collection, retention, and use of their personal information.
- 13.40 Also of concern is the reduced ability individuals have to control the use of their personal information once it is available on the internet. Indeed, it was observed at a conference of data protection and privacy professionals that:¹¹²¹

As with all information uploaded onto the internet the risks for an individual’s privacy are increased as the ability to control one’s information diminishes the longer something exists in an open and readily accessible format. For this reason the dissemination of information on the internet differs from dissemination to a group of friends in the real world. The “community” that exists on the internet includes millions of subscribers and an individual has little control over who can gain access to their personal information.

- 13.41 The ability for search engines to log information about users such as the search terms they use, their click stream data, or their locations through their IP addresses, has led to a rise in “behavioural marketing”.¹¹²² Individual pieces of information a person enters into a search engine over time, when aggregated and monitored, can build up a substantial record of personal information about an individual, including political affiliations, sexual preferences, and religious beliefs. Marketers make use of these characteristics to shape marketing practices and advertisements in a manner that will maximise their chances of profiting from consumers. Of concern is the opaque nature of practices used in behavioural marketing that result in “consumers remaining largely unaware of the monitoring of their online behaviour, the security of this information and the extent to which this information is kept confidential.”¹¹²³

1120 Electronic Privacy Information Center “Search Engine Privacy” www.epic.org/privacy/search_engine (accessed 10 December 2009). There are a range of views as to whether IP addresses are personal information within the scope of the Privacy Act. This issue is discussed in chapter 3.

1121 Resolution on Privacy Protection in Social Network Services (30th International Conference of Data Protection and Privacy Commissioners, Strasbourg, 30 October 2008).

1122 Behavioural marketing is discussed in chapter 15.

1123 Electronic Privacy Information Center “Search Engine Privacy” www.epic.org/privacy/search_engine (accessed 10 December 2009).

13.42 Researchers at the University of California at Berkeley have published a study regarding the data handling practices of popular websites and the concerns of internet users with a view to identifying the gap between users' expectations and practice, a gap they found to be a wide one.¹¹²⁴ Based on previous studies and surveys that had been conducted the researchers observed that:¹¹²⁵

- users are concerned about websites collecting information about them and using it for behavioural advertising;
- users desire control over the collection and use of information about them; and
- users lack knowledge and understanding about data collection practices and policies.

To alleviate these concerns and to give individuals more control over their personal information the researchers made the following recommendations:¹¹²⁶

- users should be entitled to see all data collected about them and who their data has been shared with;
- users should be given clear and proper notice as to who their data will be shared with and data should only be shared with prior permission;
- third party tracking should be made more transparent and browser developers should provide a function that alerts users to the presence of third party trackers;
- the Federal Trade Commission¹¹²⁷ should become more aggressive in protecting privacy on the internet;
- privacy policies should be readable for average users; and
- enhancement (buying information about users from outside sources) should be subject to user opt-in.

13.43 The Article 29 Data Protection Working Party¹¹²⁸ has also reported on data protection issues related to search engines. The group found that the collection and storage of search histories of individuals in a directly or indirectly identifiable form invokes the protection individuals are afforded under Article 8 of the European Charter of Human Rights to respect for private and family life.¹¹²⁹ Accordingly the EU Data Protection Directive applies to the processing of personal data by search engines (including IP addresses).¹¹³⁰ Essentially, the recommendations support general calls for greater transparency of information collection practices and the need for pre-informed consent to the collection of personal information. The recommendations include:

- that personal data should be retained no longer than necessary, and should only be kept in any case if there is a reason to do so;

1124 UC Berkeley, School of Information *Know Privacy* (Berkeley (CA), 2009).

1125 UC Berkeley, School of Information *Know Privacy* (Berkeley (CA), 2009) 5.

1126 UC Berkeley, School of Information *Know Privacy* (Berkeley (CA), 2009) 5.

1127 The US government regulator responsible for enforcing consumer privacy issues.

1128 The Working Party is an independent European advisory body on data protection and privacy.

1129 Article 29 Data Protection Working Party *Opinion on data protection issues related to search engines* (4 April 2008) 00737/EN WP148, 7.

1130 Article 29 Data Protection Working Party *Opinion on data protection issues related to search engines* (4 April 2008) 00737/EN WP148, 8.

- that users should be informed when they are visiting websites that use cookies,¹¹³¹ and that cookies should only be used in any case for a reasonable period of time (rather than permanently or for unnecessarily long periods);
 - that websites should provide sufficient information to users (through transparent privacy policies) to enable them to make informed choices about their internet use; and
 - that websites should allow users access to the personal information that the site holds about them, including the ability to delete and correct any erroneous information.
- 13.44 In the United Kingdom, the Information Commissioner is engaging in consultation on a code of practice to provide comprehensive, accessible guidance on the following broad areas:
- operating a privacy-friendly website;
 - rights and protections for individuals;
 - privacy choices and default settings; and
 - cyberspace and territoriality.

The code is due to be released in May 2010.¹¹³² The Information Commissioner has also released a code of practice about privacy notices, with examples of good and bad privacy notices.¹¹³³

- 13.45 The New Zealand Privacy Commissioner has also produced information about privacy notices.¹¹³⁴ The New Zealand Computer Society Code of Practice encourages information technology professionals to consider privacy issues such as privacy notices when creating websites.¹¹³⁵
- 13.46 Some search engines and websites have started to respond to concerns of privacy advocates and created tools aimed at allowing individuals to gain greater control over their personal information. One such service, known as Google Dashboard,¹¹³⁶ allows users who hold Google accounts to view a summary of any information the site holds about them and enables them to delete it if they choose to do so.¹¹³⁷ It is said that the site provides an answer to the question “what does Google know about me?”¹¹³⁸ Google claims that Dashboard gives users more transparency and control over their use of Google products, including Google search.¹¹³⁹ Tools such as this go some way towards ensuring that individuals

1131 An amendment to the EU privacy directive requires user consent to the use of cookies: “EU Adopts Law Requiring User Consent for Cookies” (10 November 2009) www.clickz.com (accessed 10 December 2009); “Browser Settings Satisfy New EU Cookie Law, says IAB” (8 December 2009) www.clickz.com (accessed 10 December 2009).

1132 Information Commissioner’s Office (UK) “Our Current Consultations” www.ico.gov.uk (accessed 27 November 2009).

1133 Information Commissioner’s Office (UK) *Privacy Notices Code of Practice* (2009).

1134 Office of the Privacy Commissioner *Questions and Answers about Layered Privacy Notices* www.privacy.org.nz (accessed 15 January 2010).

1135 New Zealand Computer Society *Information Technology Code of Practice* (2009).

1136 Google Dashboard www.google.com/dashboard (accessed 18 January 2010).

1137 The site also allows users to review and regulate information about a user created through the use of other Google products. These include Gmail, YouTube, and Google docs.

1138 <http://googlesystem.blogspot.com/2009/11/google-dashboard.html> (accessed 10 December 2009).

1139 <http://googleblog.blogspot.com/2009/11/transparency-choice-and-control-now.html> (accessed 10 December 2009).

maintain control and awareness of how their search history is tracked and recorded. Critics of Dashboard consider that although this is a step in the right direction, it should give users total ability to be anonymous from the company and advertisers in areas such as search data and online behaviour.¹¹⁴⁰

The public sector

13.47 In the US, the Center for Democracy & Technology and the Electronic Frontier Foundation have issued “open recommendations” for government agencies to balance the key role that the internet has to play in citizen engagement and the privacy of citizens who engage through the site.¹¹⁴¹ The paper recommends that agencies should only be allowed to use “Web measurement” (the analysis of internet data in the aggregate to understand and optimise web usage) if certain conditions are observed:

- Web measurement data should only be used for that purpose;
- agencies should avoid outsourcing data collection to commercial partners;
- disclosure about the use of Web measurement tools should be made in privacy policies;
- the collection of data for cross-session measurement (requiring persistent user identifiers such as persistent cookies that last across sessions) should be subject to user choice;
- individual-level data collected for measurement purposes should be retained for no more than 90 days, while elements of individual-level data that are not relevant to measurement analysis and reporting should be deleted as soon as possible after collection;
- privacy compliance procedures should be independently verified; and
- persistent tracking technologies (such as cookies) should be subject to further conditions, including a compelling need to gather the data, and appropriate privacy safeguards.

13.48 No legal controls restricting the use of cookies on government websites exist in New Zealand. At a minimum, the New Zealand Government Web Standards 2.0 require that users of government websites be informed if a site is using cookies and the implications of their use.¹¹⁴² The standards also provide that the privacy statement (which a site is required to have) should clearly state the agency’s policy regarding the collection and use of statistical information including the use of users’ IP addresses.¹¹⁴³ Similarly, the use of cookies and tracking of click stream data is not prohibited in Australia at the federal level. The Australian Privacy Commissioner’s website states that if federal government websites do use cookies and track click stream data, users are to be fully informed of this and the possible implications.¹¹⁴⁴

1140 See, for example, comments in Doug Gross “Google Releases Dashboard Privacy Tool” (6 November 2009) <http://edition.cnn.com> (accessed 24 February 2010).

1141 Center for Democracy & Technology and Electronic Frontier Foundation *Open Recommendations for the Use of Web Measurement Tools on Federal Government Web Sites* (Washington, DC, 2009).

1142 New Zealand Government *Web Standards 2.0* (Wellington, 2009).

1143 New Zealand Government *Web Standards 2.0* (Wellington, 2009).

1144 Office of the Privacy Commissioner (Cth) *Guidelines for Federal and ACT Government Websites* (Sydney, 2003).

Social networking

- 13.49 In *Privacy: Concepts and Issues*, we discussed the prevalence of social networking, particularly among young people.¹¹⁴⁵ Social networking sites such as MySpace, Bebo, and Facebook can be described as “websites that let people socialise online; send messages to one another; share interests and information; chat; meet people; and post information, photos and videos about themselves for others to look at.”¹¹⁴⁶ Social networking has been described as “the global consumer phenomenon of 2008”,¹¹⁴⁷ with social networking and blogging sites now the fourth most popular activity on the internet.
- 13.50 Social networking sites allow individuals to create a personal account that is accessible by user name and password. Accounts can usually be created after providing a name and email address but in some cases more information, including gender and date of birth details, may also be required. All other information is uploaded voluntarily by the individual user, including information such as telephone numbers and physical and email addresses. In doing so a user creates an online identity for himself or herself and gains the ability to communicate with other individuals who have similarly created their own identities on the network. Once an account is created the information is accessible to other users of the social networking site and, if users do not take the necessary steps to restrict access to their information, can be accessible to anyone using the internet. Some sites offer security settings which allow users to restrict access to others; however this is rarely the default position.
- 13.51 Social networking sites contribute to the vast wealth of personal information about individuals that is amassing on the internet.¹¹⁴⁸ A 2007 study found that of the 78 per cent of New Zealanders who use the internet, 28 percent are actively engaged in social networking every week.¹¹⁴⁹ According to another study conducted in 2008, 57.5 per cent of internet users worldwide use social networking sites.¹¹⁵⁰
- 13.52 Social networking sites are generally free to users,¹¹⁵¹ and gain much of their revenue through advertising, which appears as part of an account page accessed by the individual user. As well as providing advertisers with a marketing

1145 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) paras 5.33–5.48.

1146 Office of the Privacy Commissioner (Cth) “What Are Social Networking Sites?” www.privacy.gov.au/faq/individuals/sn-q1 (accessed 10 December 2009).

1147 Nielsen *Global Faces and Networked Places: a Nielsen Report on Social Networking's New Global Footprint* (2009) 1.

1148 For example, Facebook reports that it has more than 300 million active users worldwide, that more than 2 billion photos, and 14 million videos are uploaded onto the site each month and that more than 2 billion pieces of content (such as weblinks, news stories, blog posts, notes and photos) are shared with other users each week: “Statistics” www.facebook.com/press/info.php?statistics (accessed 10 December 2009).

1149 A Bell and others *The Internet in New Zealand 2007: Final Report* (Institute of Culture, Discourse and Communication, AUT University, Auckland, 2008) i.

1150 Study by Universal McCann Agency, 2008, cited in Trans Atlantic Consumer Dialogue “Resolution on Social Networking” (INFOSOC 39-09, London, 2009).

1151 However users of social networks may in fact “pay” through secondary uses of their personal profile data by the service providers, for example for targeted marketing: International Working Group on Data Protection in Telecommunications *Report and Guidance on Privacy in Social Network Services – Rome Memorandum* (43rd Meeting, Rome, 3–4 March 2008) 2.

platform, some sites repackage and sell the information of users to third parties for marketing and business purposes. Many sites sell this information in an anonymised or aggregated form that strips the information of individually identifiable factors.

Privacy issues

13.53 While social networking sites provide individual users with a new means of communication and opportunities to interact with others at the touch of a button, these sites carry risks for the privacy of individuals, both users and non-users, whose information is uploaded or used without consent. Social networking sites give rise to general internet-related privacy issues (discussed above) as well as additional privacy issues including:

- the fair use of personal information by social networking sites, other individuals and third party application developers;
- the potential for profiling individuals by piecing together pieces of information available on the internet;
- the sensitive nature of information uploaded by individual users with inadequate privacy settings;
- lack of knowledge amongst users about what is, and what is not, restricted from access by other users and third parties, and whether privacy policies are sufficiently transparent;
- the lack of privacy-friendly and security-enhancing default settings; and
- the particular privacy implications for certain groups such as children.

Privacy settings

13.54 Privacy settings available differ from site to site. Certain social networking sites allow individuals to choose whether or not personal information is shared with others. Some sites offer a granulated security regime whereby individuals can choose whether particular information is available to different grades or groups of people. Users may choose to allow their “friends” group access to their personal photographs, but not allow access to anyone in their “family” group. Privacy groups have voiced concern that privacy-friendly settings are often not the default settings on social networking sites.¹¹⁵² This means that an individual must actively set their security settings in a privacy-friendly manner. Some sites, such as Facebook, have taken measures to reduce the privacy risks for individual users who access their sites.¹¹⁵³

1152 Article 29 Data Protection Working Party *Opinion 5/2009 on Online Social Networking* (12 June 2009) 01189/09/EN WP163, 7.

1153 Facebook, for example, has stated that “Facebook’s privacy settings have played a central part in giving users control over who has access to their personal information by allowing them to choose the friends they accept and networks they join... In addition ... users are given extensive and precise controls that allow them to choose who sees what among their networks and friends, as well as tools that give them the choice to make a limited set of information available to search engines and other outside entities.” Office of the Privacy Commissioner of Canada *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc* (PIPEDA Case Summary #2009-008, Ottawa, 2009) para 66.

Information sharing

- 13.55 The underlying premise of social networking sites is the sharing of information with others. When information is uploaded onto the internet, without control, this can be viewed, downloaded, manipulated and collected by people worldwide. Unauthorised release of this information can be harmful to the individual concerned.¹¹⁵⁴ Employers, for example, have been known to access social networking pages before hiring prospective staff, and decline certain applicants on the basis of what they find. A Canadian woman is reported to have lost her long term sickness benefit due to her insurance company discovering photographs on Facebook that suggested she did not have the injury she claimed to have.¹¹⁵⁵ Social networking sites are now also being monitored by debt collection agencies to search for individuals who have disappeared leaving large debts.¹¹⁵⁶
- 13.56 As we noted in *Privacy: Concepts and Issues*, the privacy principles do not apply to the use and disclosure of personal information that is contained in or sourced from “a publicly available publication”,¹¹⁵⁷ defined as meaning “a magazine, book, newspaper, or other publication that is or will be generally available to members of the public; and includes a public register.” Whether information posted on a social networking site amounts to a publication that is generally available to members of the public may depend on the privacy settings involved.
- 13.57 As well as divulging one’s own personal information on social networking sites, the personal information of other people is increasingly being uploaded and being made available without consent, for example, by uploading photographs or written postings that disclose information about other people.¹¹⁵⁸ An individual affected by someone else’s disclosure, if it is particularly serious, may be able to bring a civil claim for a breach of privacy against the individual who uploaded the personal information.¹¹⁵⁹
- 13.58 There is also the possibility that an affected individual could make a complaint to the Privacy Commissioner. However, as we noted in *Privacy: Concepts and Issues*,¹¹⁶⁰ section 56 of the Privacy Act provides that the privacy principles do not apply in respect of personal information collected or held by an individual “solely or principally for the purposes of, or in connection with, that individual’s personal, family, or household affairs.” The primary users of social networking sites are generally individuals who do so to share information with acquaintances,

1154 In *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) paras 6.35–6.40 we noted the particular issues that arise with images on the internet. See also David V Richards “Posting Personal Information on the Internet: A Case for Changing the Legal Regime Created by § 230 of the Communications Decency Act” (2007) 85 Tex L Rev 1321.

1155 “Depressed woman loses benefits over Facebook photos” (21 November 2009) *CBC News* www.cbc.ca (accessed 10 December 2009).

1156 John Silvester “Policing in the internet age” (16 November 2009) www.stuff.co.nz (accessed 10 December 2009).

1157 New Zealand Law Commission *Privacy: Concepts and Issues*, (NZLC SP19, Wellington, 2008) para 6.43.

1158 See New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) para 6.33.

1159 For discussion of the tort of disclosure of private facts, see New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC IP14, Wellington, 2009).

1160 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) para 6.43.

friends and family, although there are sites used for professional networking. Section 56 may therefore limit the extent to which the privacy principles apply in this context.¹¹⁶¹

Third party access

- 13.59 As well as providing a basis for sending messages and uploading photographs, some social networking sites provide third party applications for users. Third party applications are tools accessible through the social networking platform for the enjoyment and benefit of users. These include games and quizzes, match-making tools, horoscopes, birthday calendars, count-down timers, and virtual pets. In the case of Facebook, the website states that it has more than one million developers and entrepreneurs from more than 180 countries who develop applications for the site and that more than 350,000 applications currently exist on the site.¹¹⁶² One concern is the ability of developers of third party applications to access without notice the personal information of those who use the applications.
- 13.60 There is also concern regarding third party use of personal information generally, whether information is obtained through third party applications, with the authorisation of non-transparent privacy policies, through malicious acts to gain access to supposedly secure information, or through unauthorised use more generally, such as unauthorised use of information posted by a user's friends. Personal data published on social networking sites can be used by third parties or other users to create profiles for a wide variety of purposes, including commercial purposes, and major risks include identity theft,¹¹⁶³ financial loss, loss of business or employment opportunities and physical harm.¹¹⁶⁴

Research and policy responses

- 13.61 In response to privacy concerns relating to social networking, several bodies have conducted studies and issued recommendations for social networking sites about how they can protect the privacy interests of users and comply with privacy laws in various countries.
- 13.62 A resolution on privacy protection in social network services was passed at the 2008 Conference of Data Protection and Privacy Commissioners, which contained a number of recommendations for providers and users of social networking services.¹¹⁶⁵ The Conference considered that “providers of social network services have a special responsibility to consider and act in the interests of the individuals using social networks.”¹¹⁶⁶ To meet the requirements of data protection laws, it resolved that that social network services should:

1161 See discussion of section 56 in chapter 5.

1162 Facebook “Statistics” www.facebook.com/press/infor.php?/statistics (accessed 10 December 2009).

1163 Identity theft is discussed in chapter 17.

1164 Article 29 Data Protection Working Party *Opinion 5/2009 on Online Social Networking* (12 June 2009) 01189/09/EN WP163.

1165 Resolution on Privacy Protection in Social Network Services (30th International Conference of Data Protection and Privacy Commissioners, Strasbourg, 30 October 2008).

1166 Resolution on Privacy Protection in Social Network Services (30th International Conference of Data Protection and Privacy Commissioners, Strasbourg, 30 October 2008) 3.

- respect the privacy standards of the countries where they operate their services;
 - provide information to users about the use of their information by the social network, privacy and security risks, as well as guidance on how users should handle their own information and the information of other people on the social networking site;
 - improve user control over profile data and secondary use of profile and traffic data (including by third party developers);
 - offer privacy-friendly default settings;
 - offer pseudonymous profiles as an option;
 - prevent bulk downloading of profile data by third parties; and
 - offer non-indexability of profiles by search engines as a default setting.
- 13.63 The Article 29 Data Protection Working Party has made a series of further recommendations, including that:¹¹⁶⁷
- sites should contain a link to a complaints body responsible for privacy issues in the country concerned; and
 - sites should maintain policies to retain data on inactive users for finite periods and agree to delete the data of abandoned accounts.

The Working Party found much social networking will fall within the “household exemption” to the Data Protection Directive;¹¹⁶⁸ however, where user activities extend beyond a purely personal or household activity, for example, to advance commercial, charitable or political goals, the exception does not apply, and data protection restrictions will apply to the use of personal information derived from social networking sites. The Working Party suggested that a high number of contacts could be an indication that the exception does not apply.¹¹⁶⁹

- 13.64 A resolution on social networking was passed by the Trans Atlantic Consumer Dialogue (TACD), a forum of US and EU consumer organisations, resolving that US and EU governments should pass legislation regulating social networks; improve co-operation and enforcement; and raise awareness of privacy risks. The TACD also resolved that social network operators should integrate privacy and security by design; enable consumers to remain “masters of their data”; develop industry and ethical codes; and provide advertisement and tracking-free versions.¹¹⁷⁰
- 13.65 In 2009 a set of “Safer Social Networking Principles” were signed between the European Commission and a number of social networking sites including Facebook, MySpace, and Bebo. The principles were developed to provide good practice guidelines (such as default privacy settings) to providers of social networking and interactive sites (such as Google) with a particular view to minimising harms to children and young people.

1167 Article 29 Data Protection Working Party *Opinion 5/2009 on Online Social Networking* (12 June 2009) 01189/09/EN WP163, 12–13.

1168 The New Zealand equivalent is the “domestic affairs” exemption in section 56 of the Privacy Act.

1169 Article 29 Data Protection Working Party *Opinion 5/2009 on Online Social Networking* (12 June 2009) 01189/09/EN WP163, 6.

1170 Trans Atlantic Consumer Dialogue “Resolution on Social Networking” (INFOSOC 39-09, London, 2009).

- 13.66 In 2008 the Privacy Commissioner of Canada commenced an investigation into the practices and policies of Facebook in response to a complaint made by the Canadian Internet Policy and Public Interest Clinic.¹¹⁷¹ The issues involved included the site's default privacy settings, collection and use of users' personal information for advertising purposes, disclosure of users' personal information to third party application developers, and collection and use of non-users' personal information
- 13.67 The Commissioner's Office issued a report including 20 recommendations for changes to Facebook's practices to comply with the privacy laws of Canada. Facebook ultimately agreed to all of the recommendations made and undertook to change its global policies and practices to comply,¹¹⁷² including:
- allowing individual users to retain more control over what information they disclose to third party applications;
 - making changes to account deactivation and deletion terms and practices;
 - making provision for the accounts of deceased users; and
 - changes that protect the privacy interests of non-users.
- 13.68 Facebook has also responded to pressure from users by altering information retention and sharing practices and improving privacy controls. The site now gives members comment and voting rights over how the site is governed.¹¹⁷³

CLOUD COMPUTING

- 13.69 Cloud computing describes the trend towards accessing computing and storage facilities from service providers on the internet, instead of using packaged software, and dedicated hard drives or network servers:¹¹⁷⁴

Cloud computing represents a new way to deploy computing technology to give users the ability to access, work on, share, and store information using the Internet. The cloud itself is a network of data centers – each composed of many thousands of computers working together – that can perform the functions of software on a personal or business computer by providing users access to powerful applications, platforms, and services delivered over the Internet.

The result of this trend is that “We are using less data and software that sit on our hard-drive and spending more time in our web browsers accessing data and applications that stream through the web.”¹¹⁷⁵ Data stored in the cloud can include information contained in word processing documents and other business documents, employee records, health information, tax and accounting records, schedules, calendars and contacts.¹¹⁷⁶

1171 Office of the Privacy Commissioner of Canada *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc* (PIPEDA Case Summary #2009-008, Ottawa, 2009).

1172 Office of the Privacy Commissioner of Canada “Facebook agrees to address Privacy Commissioner's concerns” (27 August 2009) News Release.

1173 Nielsen *Global Faces and Networked Places: a Nielsen Report on Social Networking's New Global Footprint* (2009) 9.

1174 Jeffrey F Rayport and Andrew Heyward *Envisioning the Cloud: the Next Computing Paradigm* (Marketspace, 2009) ii.

1175 “Microsoft after Bill Gates” (26 June 2008) *The Economist*, quoted in Jeffrey F Rayport and Andrew Heyward *Envisioning the Cloud: the Next Computing Paradigm* (Marketspace, 2009) 5.

1176 Shari Claire Lewis “Cloud Computing Brings New Legal Challenges” (8 July 2009) *New York Law Journal*.

- 13.70 The advantages of cloud computing include its convenience and versatility, with a shift from using an anchored, traditional personal computer terminal for internet services to using a range of smaller portable computing devices for internet access (such as internet capable cellphones).¹¹⁷⁷
- 13.71 Cloud computing can involve individuals using cloud services in relation to their personal information, as well as businesses using cloud services for their operations that may include the handling of the personal information of their employees, clients or customers. According to the Electronic Privacy Information Center, as of September 2008, 69 per cent of Americans were using webmail services, storing data online and otherwise using software programmes such as word processing applications whose functionality is located on the web.¹¹⁷⁸ Popular cloud services used by individuals include web mail, social networking sites, photo sharing and video viewing sites such as YouTube.¹¹⁷⁹
- 13.72 Cloud computing is of growing importance to businesses as it offers efficiencies and cost savings from outsourcing IT functions such as computing and data storage through access to the significant capacity of data centres.¹¹⁸⁰ Users can access this computing power in a similar way to utilities such as electricity, and pay for the service they use, thereby saving the cost of unused capacity: “A key underlying premise of the economic model driving cloud computing is that sharing resources creates efficiencies.”¹¹⁸¹
- 13.73 The term “cloud computing” covers a range of different services that are organised in different ways.¹¹⁸² The foundation of all Cloud services is Infrastructure as a Service (IaaS):¹¹⁸³

The capability provided to the consumer is to rent processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer

1177 See Jonathan Zittrain “Lost in the Cloud” (20 July 2009) *New York Times* www.nytimes.com (accessed 22 July 2009).

1178 Electronic Information Privacy Center “In re Google and Cloud Computing” <http://epic.org/privacy/cloudcomputing/google> (accessed 17 June 2009).

1179 Jeffrey F Rayport and Andrew Heyward Jeffrey F Rayport and Andrew Heyward *Envisioning the Cloud: the Next Computing Paradigm* (Marketspace, 2009) i.

1180 For example it has been estimated that a proposed move to Google Apps by the Los Angeles City Council would save about US\$13 million in software licensing and personnel costs over a 5 year period: Jaikumar Vijayan “Google Defends Google Apps Security” (28 July 2009) *ComputerWorld* www.computerworld.com (accessed 31 July 2009). See also the NZ Post three-year cloud computing contract for Google email and messaging that will save NZ\$2 million: Anthony Doesburg “NZ Post Signs Up for Cloud Service” (21 July 2009) *New Zealand Herald* Auckland www.nzherald.co.nz (accessed 23 July 2009).

1181 Jim Reavis, Pam Fusco and Josh Zachry “Data Center Operations” in Cloud Security Alliance *Security Guidance for Critical Areas of Focus in Cloud Computing* (2009) 59.

1182 The US National Institute of Technology and Standards has produced a draft working definition of cloud computing as “a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” The five key characteristics are (i) on-demand self-service, (ii) ubiquitous network access (iii) location independent resource pooling (iv) rapid elasticity and (v) measured service: see Katten Muchin Rosenman LLP and UHY Advisors FLVS Inc *Cloud Computing: Practice Safe SaaS: Don't Lose Your Head (or Data) in the Clouds* (2009).

1183 Christofer Hoff “Cloud Architecture” in Cloud Security Alliance *Security Guidance for Critical Areas of Focus in Cloud Computing* (2009) 17.

does not manage or control the underlying cloud infrastructure but has control over operating systems, deployed applications, and possibly select networking components (e.g. firewalls, load balancers).

This foundation can be built on by other delivery models such as Platform as a Service (PaaS)¹¹⁸⁴ and Software as a Service (SaaS).¹¹⁸⁵

13.74 In addition, there are four primary ways in which Cloud services can be deployed and characterised:¹¹⁸⁶

- Private Clouds, which are dedicated to a single organisation, either on their premises or off their premises;
- Public Clouds, which are provided to a single organisation or multiple organisations, generally off premises;
- Managed Clouds where the physical infrastructure is owned by or physically located in an organisation's data centre with aspects of management and security controlled by the service provider; and
- Hybrid Clouds which are a combination of public and private clouds.

13.75 The rapid growth in these services has given rise to some security glitches that have allowed private information to be shared without authority.¹¹⁸⁷ Use of these services may involve a privacy trade-off where a service provider offers a free service such as storage, while retaining the right to mine user data for market research or for the purposes of targeted advertising.¹¹⁸⁸ In some cases, users have found it difficult to regain or erase their data when they wish to terminate their use of one of these services.

13.76 Because cloud computing can involve the transfer of data and potentially a reduction or loss of control by the organisation which is the ostensible custodian of that information, it gives rise to a range of issues,¹¹⁸⁹ requiring prior risk assessment and due diligence, including consideration of the contractual terms that will govern the arrangement between the user and cloud service provider.

1184 PaaS is the capability to deploy onto the cloud infrastructure consumer-created applications using programming languages and tools supported by the provider: Christofer Hoff "Cloud Architecture" in Cloud Security Alliance *Security Guidance for Critical Areas of Focus in Cloud Computing* (2009) 17.

1185 SaaS is the capability to use the provider's applications running on a cloud infrastructure and accessible from various client services through a thin client interface such as a Web browser: Christofer Hoff "Cloud Architecture" in Cloud Security Alliance *Security Guidance for Critical Areas of Focus in Cloud Computing* (2009) 17.

1186 Christofer Hoff "Cloud Architecture" in Cloud Security Alliance *Security Guidance for Critical Areas of Focus in Cloud Computing* (2009) 19.

1187 See Jason Kincaid "The Sorry State of Online Privacy" (26 April 2009) *Washington Post* www.washingtonpost.com (accessed 28 April 2009). See also Electronic Privacy Information Center "In the Matter of Google, Inc. and Cloud Computing Services before the Federal Trade Commission, Complaint and Request for Injunction, Request for Investigation and Other Relief" (17 March 2009), requesting an investigation into Google's cloud computing services to determine "the adequacy of the privacy and security safeguards regarding the storage of personal information on its Cloud Computing Services".

1188 James Keller "Web-based Computing Spurs Privacy Concerns" (4 March 2009) *The Canadian Press* www.theglobeandmail.com (accessed 17 March 2009).

1189 One US law firm describes security, privacy and eDiscovery as the three biggest concerns about cloud computing: Katten Muchin Rosenman LLP and UHY Advisors FLVS Inc *Cloud Computing: Practice Safe SaaS: Don't Lose Your Head (or Data) in the Clouds* (2009).

Privacy is one of the sets of issues that arise in relation to the use of cloud computing. The type of issue that arises and its significance will depend to some extent on the type of cloud computing that is being considered.

13.77 One tool to work through the range of potential privacy issues is a Privacy Impact Assessment. Some of the potential privacy issues include:¹¹⁹⁰

- whether the use of cloud services by an agency holding personal information will involve an activity that is regulated by the Privacy Act (such as use or disclosure) and whether any of the exceptions apply;
- whether the use of cloud services is consistent with the organisation's privacy policy or whether people need to consent to their data being transferred to a cloud computing environment;
- assessing where the data will be located (if possible) and which privacy laws will apply;¹¹⁹¹
- assessing the terms of the cloud provider's privacy statement, whether it is liable to be changed and whether it gives the cloud provider rights in relation to the cloud user's information;
- whether the cloud provider outsources any aspects of the service to other businesses, whether there is any potential for further cross-border transfers of the data and whether this impacts on the relevant privacy regulation;
- whether the data in the cloud will be held separately or comingled with the data of other cloud users;
- the limits on the scope of what the cloud provider is permitted to do with the data and whether there are any circumstances in which the service provider can access or use the data (that is, for commercial purposes such as marketing through behavioural targeting);
- whether the cloud provider can use or access transactional, relationship or metadata associated with the data being processed by the cloud service;¹¹⁹²
- the circumstances in which the data can be obtained by domestic or overseas law enforcement agencies or other third parties;
- whether the cloud service poses any risks to the security or integrity of the data being processed;
- the levels of security and encryption,¹¹⁹³ including the security of data in transit, taking account of potential risks from the cloud provider, other users of the same cloud services, and cyber criminals;
- how people will be able to access and correct data about them, once it resides in a cloud environment;
- how data will be disposed of or archived once it is no longer needed;
- how the cloud user can monitor or audit the arrangement to check that the information is being held securely; and

1190 See generally Cloud Security Alliance *Security Guidance for Critical Areas of Focus in Cloud Computing* (2009).

1191 See Jeffrey F Rayport and Andrew Heyward *Envisioning the Cloud: the Next Computing Paradigm* (Marketspace, 2009) 39.

1192 Robert Gellman *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing* (World Privacy Forum, 2009) 21.

1193 See for example the letter by 38 researchers and academics to Google expressing concern that web-based encryption is not used as a default setting in certain aspects of its cloud based services: Electronic Information Privacy Center <http://epic.org/privacy/cloudcomputing/google> (accessed 17 June 2009).

- what happens to the data on termination of the cloud service, for example once the contract expires, if the cloud provider goes out of existence, if the cloud service provider unexpectedly terminates the arrangement, or if there is a merger or takeover affecting the cloud provider.

Privacy Act framework

- 13.78 The following Privacy Act principles and provisions are relevant to New Zealand agencies using cloud computing services.
- 13.79 Section 3(4) provides that where an agency (such as a cloud service provider) holds information solely for the purpose of safe custody or processing the information on behalf of another agency, and does not use or disclose the information for its own purposes, the information is deemed to be held by the agency engaging the service provider. This means that, if the cloud computing provider does not use or disclose the information for its own purposes, the agency engaging processing or custodial services remains responsible for the data under the Privacy Act, and the cloud service provider does not attract obligations under the Privacy Act. This incentivises an outsourcing agency to use a reputable service provider and ensure rigorous contractual terms to minimise the risk that the outsourcing agency will be held responsible for any breach by the service provider.
- 13.80 Section 10 confirms that principles 5 to 11 continue to apply to information that is held outside New Zealand by an agency (which will include information held by a cloud custodian or processor of information that does not use or disclose the information for its own purposes under section 3(4)).
- 13.81 Where it is necessary to give personal information to a person in connection with the provision of a service to the agency, principle 5(b) requires that everything reasonably within the power of the outsourcing agency is done to prevent unauthorised use or disclosure.¹¹⁹⁴ One way to achieve this is through appropriate contractual arrangements.
- 13.82 Principle 10 contains no specific exception dealing with data processing or the outsourcing of information-handling, suggesting that where any processing or outsourcing amounts to “use” it requires the consent of those people to whom the personal information relates unless one of the other exceptions applies. However where there is no “use” of the information (such as storage services), principle 10 would not be engaged.
- 13.83 Likewise, principle 11 contains no specific exception dealing with processing or the outsourcing of information-handling, suggesting that where any processing or outsourcing amounts to “disclosure” to the cloud service provider, it requires the consent of those people to whom the personal information relates, unless one of the other exceptions applies. However where there is no “disclosure” of the information (such as storage services with no access rights, or secure automated processing), principle 11 would not be engaged.

¹¹⁹⁴ One issue is whether “unauthorised” in this context means (i) unauthorised by the agency engaging the service, (ii) unauthorised by the persons to whom the information relates, and thus requires consent, or (iii) unauthorised under privacy principles 10 and 11. Reference to principle 5(a)(ii) suggests that the intended interpretation is unauthorised by the agency engaging the service.

Cross-border issues

- 13.84 Because cloud computing will often involve data being stored in data centres offshore, it raises issues of trans-border data flows. Depending on the precise details of how an agency uses cloud computing, in cases where the provider of cloud computing services holds or processes personal information on behalf of a New Zealand agency, without using or disclosing it for the cloud provider's own purposes, section 3(4) would apply and the information held in the cloud would be deemed to be held by the New Zealand agency. The New Zealand agency would therefore remain accountable and responsible for ensuring that the privacy principles are observed.
- 13.85 However, where a cloud computing arrangement allows for information sharing between the user agency and the cloud service provider,¹¹⁹⁵ this would be outside the scope of section 3(4) and the New Zealand agency would not necessarily remain accountable for the further use and disclosure of the information by the cloud service provider, except for the obligation under principle 5(b) to ensure the prevention of unauthorised use and disclosure. Except for a complaint against a user agency under principle 5(b), complaints of misuse of personal information by the cloud service provider would have to be made against that provider (which may be an offshore entity) rather than the New Zealand agency. The issues associated with trans-border data flows and options for reform are discussed in chapter 14.¹¹⁹⁶
- 13.86 It is also worth noting that where agencies and organisations that are exempt from the privacy principles¹¹⁹⁷ use cloud services to store or process personal information, they may do so without regard to the requirements of the Privacy Act.

DEEP PACKET INSPECTION

- 13.87 Deep packet inspection (DPI) is a form of computer network packet filtering¹¹⁹⁸ that can assist internet service providers (ISPs) to monitor traffic loads and manage network performance.¹¹⁹⁹ DPI can also filter out spam and viruses. The Canadian Privacy Commissioner has noted that DPI is not a new technology, as it has been used for some time for network security purposes.¹²⁰⁰ What is new, however, is how DPI can potentially be deployed by ISPs in traffic management.¹²⁰¹ The new potential of DPI is being hotly debated in international privacy circles because of its privacy implications. A major concern is that because DPI involves not just the inspection of traffic data (such as email addresses) but also content data (such as the content of emails),¹²⁰² it therefore potentially allows the

1195 The information sharing would need to comply with the requirements of principle 11.

1196 See also Patrick Kershaw "Telephony the Answer for Tough Times?" (23 April 2009) *The Independent London*.

1197 Privacy Act 1993, s 2(1), definition of "agency."

1198 Including, for example, "packet sniffers."

1199 See Graham Finnie *ISP Traffic Management Technologies: The State of the Art* (Report prepared on behalf of the Canadian Radio-television and Telecommunications Commission, 2009).

1200 Office of the Privacy Commissioner of Canada *Report of Findings: Assistant Commissioner Recommends Bell Canada Inform Customers About Deep Packet Inspection* (PIPEDA Case Summary #2009-010, Ottawa, 2009) para 8.

1201 See generally See Paul Ohm "The Rise and Fall of Invasive ISP Surveillance" [2009] U Ill L Rev 1417.

1202 DPI has been described as the equivalent of opening people's mail: Saul Hansell "The Economics of Snooping on Internet Traffic" (25 March 2009) <http://bits.blogs.nytimes.com> (accessed 24 August 2009), attributing this comment to Tim Berners-Lee.

monitoring and collection of customers' internet activity in its entirety.¹²⁰³ Another major concern is the potential for DPI to be used for the purposes of targeted advertising.

- 13.88 A number of factors have given rise to the potential for DPI. These include the current use of network monitoring by ISPs to monitor network threats and viruses, improvements in network monitoring technology, the search by broadband ISPs for new sources of revenue, incentives from online advertisers, the successful adoption of behavioural targeting by other internet players such as search engines (providing a commercial model for ISPs to emulate), and the push from copyright enforcers to require ISPs to use network monitoring to control intellectual property infringements.¹²⁰⁴
- 13.89 Several issues that we have discussed in relation to other aspects of this privacy Review are brought together in DPI including:
- the interception of electronic messages;¹²⁰⁵
 - the collection of internet data (discussed above); and
 - behavioural targeting.¹²⁰⁶

Policy responses

- 13.90 DPI has been the subject of review, both specifically and in the context of wider enquiries into network neutrality and the open internet, in the European Union, the United States and Canada. The European Commission initiated an investigation into British Telecom trials of ad-serving technology developed by Phorm that monitored users' web-surfing behaviour.¹²⁰⁷
- 13.91 In the United States, 15 web-users sued NebuAd and six ISPs for violating their privacy by deploying a behavioural targeting platform that used DPI technology to monitor users' Web activity. DPI has also attracted congressional attention with hearings before the subcommittee on Communications, Technology and the Internet.¹²⁰⁸
- 13.92 The Federal Communications Commission (FCC) has issued a notice of proposed rulemaking in relation to preserving open internet broadband industry practices.¹²⁰⁹ The Notice proposes the codification of a number of principles, one of which relates to transparency, requiring disclosure of internet management practices.

1203 See Electronic Privacy Information Center "Deep Packet Inspection and Privacy" <http://epic.org/privacy/dpi> (accessed 17 June 2009). See also Center for Democracy and Technology "The Privacy Implications of Deep Packet Inspection" (23 April 2009) Statement of Leslie Harris, President and Chief Executive of Center for Democracy and Technology before the House Subcommittee on Communications, Technology and the Internet.

1204 See generally Paul Ohm "The Rise and Fall of Invasive ISP Surveillance" [2009] U Ill L Rev 1417.

1205 See New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC R113, Wellington, 2010) chapter 3 and appendix A.

1206 Behavioural targeting is discussed in chapter 15.

1207 See Paul Ohm "The Rise and Fall of Invasive ISP Surveillance" (2009) U Ill L Rev, 1417 paras 17–18.

1208 Saul Hansell "Congress Begins Deep Packet Inspection of Internet Providers" (24 April 2009) <http://bits.blogs.nytimes.com> (accessed 8 July 2009).

1209 Federal Communications Commission "In the Matter of Preserving the Open Internet Broadband Industry Practices: Notice of Proposed Rulemaking" (22 October 2009).

- 13.93 The Canadian Radio-television and Telecommunications Commission (CRTC) has conducted a review of internet traffic management practices. In a submission to the review, the Canadian Privacy Commissioner compiled the following list of privacy questions raised by DPI:¹²¹⁰
- What are the appropriate uses of DPI?
 - When should DPI be activated and under what authority?
 - What information management processes and controls should be used by organisations deploying DPI technology, or third parties with access to this information?
 - What should be required in relation to:
 - informing the customer about the use of DPI;
 - customer choices regarding use of DPI for security; and
 - customer choices regarding use of DPI for selling profiling data to third parties?
 - What information that is potentially examinable by DPI constitutes personal information and is, therefore, subject to the protections of privacy legislation?
 - Should consideration be given to the appropriateness of underlying design decisions as the exploitation of weaknesses gives rise to the need for DPI?
- 13.94 While noting that privacy concerns relate to the *potential* use of technologies used for internet traffic management practices rather than their current use, the CRTC concluded that it would be appropriate to impose a higher standard than required under PIPEDA to ensure a higher degree of privacy protection for telecommunications customers. The Commission has directed that:¹²¹¹
- ISPs are not to use personal information collected for the purposes of traffic management for other purposes, and are not to disclose such information; and
 - ISPs are to disclose internet traffic management practices to customers clearly and prominently on their websites.
- 13.95 The Canadian Privacy Commissioner has devoted a section of the Office’s website to issues associated with DPI¹²¹² and has investigated a complaint about the DPI practices of Bell Canada.¹²¹³ The Privacy Commissioner rejected complaints that Bell was collecting personal information about customers without their consent and that Bell was gathering more information than it needed to manage its network. However the Privacy Commissioner did require Bell to change its service agreements, and the Frequently Asked Questions section of its website, to notify customers that it collects and retains personal information through use of its DPI technology.¹²¹⁴

1210 Office of the Privacy Commissioner of Canada “Review of the Internet Traffic Management Practices of Internet Service Providers” (Submission to the Canadian Radio-television and Telecommunications Commission, 2009).

1211 Canadian Radio-television and Telecommunications Commission “Review of the Internet Traffic Management Practices of Internet Service Providers” www.crtc.gc.ca (accessed 20 November 2009).

1212 Office of the Privacy Commissioner of Canada *Deep Packet Inspection: A Collection of Essays from Industry Experts* <http://dpi.priv.gc.ca> (accessed 8 December 2009).

1213 Office of the Privacy Commissioner of Canada *Report of Findings: Assistant Commissioner Recommends Bell Canada Inform Customers About Deep Packet Inspection* (PIPEDA Case Summary #2009-010, Ottawa, 2009).

1214 Office of the Privacy Commissioner of Canada *Report of Findings: Assistant Commissioner Recommends Bell Canada Inform Customers About Deep Packet Inspection* (PIPEDA Case Summary #2009-010, Ottawa, 2009).

New Zealand regulatory framework

13.96 Deep packet inspection is potentially regulated in New Zealand by interception offences in the Crimes Act.¹²¹⁵ Under the civil law, the collection of telecommunications information is governed by the Telecommunications Information Privacy Code 2003 which modifies the application of the privacy principles in relation to telecommunications.

Telecommunications Information Privacy Code

13.97 “Telecommunication” is given the same meaning as under the Telecommunications Act 2001:¹²¹⁶

The conveyance by electromagnetic means from one device to another of any encrypted or non-encrypted sign, signal, impulse, writing, image, sound, instruction, information, or intelligence of any nature, whether for the information of any person using the device or not.

13.98 The Code applies to information about an identifiable individual that is:¹²¹⁷

- subscriber information (personal information about a subscriber which is obtained by an agency at the time the subscriber subscribes or during the term of the contractual relationship);
- traffic information (call associated data¹²¹⁸ and any other dialling or signalling information generated as the result of making a telecommunication); and
- the content of a telecommunication.

The Code extends to ISPs.¹²¹⁹

13.99 The use of DPI by ISPs is likely to involve the collection of telecommunications directly from their customers but because of the range of exceptions to the notice requirement (such as that there will be no prejudice to the customer’s interests, or notification is not practicable, or the information will not be used in a form

1215 Crimes Act 1961, s 216B(1), although s 216B(5) contains an exception for employees of internet service providers carrying out network maintenance services.

1216 Telecommunications Act 2001, s 5.

1217 Telecommunications Information Privacy Code 2003, cl 4(1).

1218 Call associated data is defined in the Telecommunications Information Privacy Code 2003, cl 3 as follows:

- (a) dialling or signalling information
 - (i) generated as a result of the making of the telecommunication (whether or not the telecommunication is received successfully); and
 - (ii) that identifies the origin, direction, destination, or termination of the telecommunication; and
- (b) without limiting the generality of paragraph (a), includes any of the following information:
 - (i) the number from which the telecommunication originates;
 - (ii) the number to which the telecommunication is sent;
 - (iii) if the telecommunication is diverted from one number to another number, those numbers;
 - (iv) the time at which the telecommunication is sent;
 - (v) the duration of the telecommunication;
 - (vi) if the telecommunication is generated from a mobile telephone, the point at which the telecommunication first enters a network; but
- (c) does not include the content of the telecommunication.

1219 Telecommunications Information Privacy Code 2003, cl 4(2).

that identifies the customer), there may be an issue as to whether customers would always get notice about DPI. There is also a specific exception to notice where the collection is for the purpose of preventing or investigating an action or threat that may compromise network or service security or integrity.¹²²⁰

- 13.100 Where the telecommunications information of non-customers (such as email recipients) is collected incidentally through DPI of the internet activity of ISP customers, there is no particular notification requirement. Rule 2 requires telecommunications information to be collected directly from the individual concerned; however, this is not required if not reasonably practicable.¹²²¹ There is also an express exception for the collection of traffic information.¹²²²
- 13.101 The use and disclosure of telecommunications information for a purpose other than the purpose for which it was collected is limited under rules 10 and 11. However, the use and disclosure of information collected through DPI for an intended purpose such as behavioural targeting is not expressly restricted.
- 13.102 The Code expressly permits ISPs to monitor call associated data where necessary to investigate an action that may threaten network security or integrity (subject to section 107 of the Telecommunications Act which prohibits the use of telephone analysers, although there is an exception for maintenance of the network) but this does not extend to content data.¹²²³
- 13.103 Depending on its extent, the collection of personal information using DPI may be unlawful (and, indeed, criminal¹²²⁴) or unfair, or may intrude to an unreasonable extent into the personal affairs of an individual, which would make it in breach of rule 4.

LOCATION TECHNOLOGIES

- 13.104 In *Privacy: Concepts and Issues*, we outlined developments in relation to location technologies.¹²²⁵ The global positioning system (GPS) transmits satellite signals to a receiver, making it possible to determine where a person is at any given time, or where a person has been, by accessing location data. Location data is also generated by cellphones, payment and entry systems such as transit swipe cards (for example, Wellington's Snapper cards), electronic tolling devices and electronic swipe cards for doors. Companies continue to develop location-based services for the internet. For example, Google Latitude allows users to share their cellphone location with friends via the internet or smart phone.¹²²⁶
- 13.105 In the report for stage 3 of our Review we recommended the creation of a new criminal offence where someone uses a tracking device to determine someone else's location without consent, and we gave examples of scenarios that the

¹²²⁰ Telecommunications Information Privacy Code 2003, cl 5, rule 3(4)(b)(iii).

¹²²¹ Telecommunications Information Privacy Code 2003, cl 5, rule 2((2)(f).

¹²²² Telecommunications Information Privacy Code 2003, cl 5, rule 2((2)(h).

¹²²³ Telecommunications Information Privacy Code 2003, cl 5, rule 4.

¹²²⁴ For example if it involves the "interception of a private communication" that does not fall within the service provider exception: Crimes Act 1961, s 216B(5).

¹²²⁵ New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) paras 6.81–6.89.

¹²²⁶ See, eg, Ian Paul "Google Latitude Services Lets You Track Your Friends: How It Works" (5 February 2009) *PC World*; David Coursey "Spy on Your Workers with Google Latitude" (5 February 2009) *PC World* www.peworld.com (accessed 24 February 2010).

offence is intended to cover.¹²²⁷ The proposed offence would cover the active use of a device to produce location data without the consent of the target of the surveillance and would prohibit the disclosure of information thus obtained, but would not otherwise prohibit the handling and use of location data.

- 13.106 The development of location technologies has led to concerns about preserving spatial (or “locational”) privacy. The Electronic Frontier Foundation has called for location tracking systems to be built with privacy as a central component of their design. It is possible to create systems that do not in fact collect locational data, whilst still delivering the service they are designed to deliver.¹²²⁸
- 13.107 The European Union Directive on Privacy and Electronic Communications deals explicitly with location data in the electronic communications sector.¹²²⁹ The Directive prohibits the processing of location data that has not been anonymised without the consent of the user of the service. It also requires service providers to inform users, before obtaining their consent, of the type of location data to be processed, the purpose and duration of the proposed processing, and whether the data will be transmitted to a third party. Users must be given the opportunity to withdraw their consent at any time. Processing of the data must be restricted to that which is necessary for the purpose of providing the service.¹²³⁰

RADIO FREQUENCY IDENTIFICATION

- 13.108 In *Privacy: Concepts and Issues*, we outlined developments in relation to radio frequency identification (RFID),¹²³¹ which raises some similar issues to location technologies. RFID technology can be used for a variety of purposes. It was first developed as a mechanism for inventory control to replace barcodes. Current uses of RFID in New Zealand include office swipe cards, the new biometric passport and microchipping of dogs. There are concerns about its potential to track people by the tagged objects they carry or potentially by means of a chip implanted under the skin.¹²³² Privacy concerns about RFID also arise from the ability for RFID data to be aggregated with other information so as to create detailed profiles about consumers, and the ability to clone RFID chips.

1227 New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC R113, Wellington, 2010) paras 3.46–3.54, recommendation 8.

1228 Andrew J Blumberg and Peter Eckersley *On Locational Privacy, and How to Avoid Losing it Forever* (Electronic Frontier Foundation, San Francisco, 2009).

1229 European Parliament and Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201.

1230 European Parliament and Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201, cited in Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) para 9.88.

1231 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) paras 6.71–6.80. See also New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC IP14, Wellington, 2009) paras 10.72–10.74.

1232 See Ian Kerr “The Internet of People? Reflections on the Future Regulation of Human-Implantable Radio Frequency Identification” in Ian Kerr, Valerie Steeves and Carole Lucock (eds) *Lessons From the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Oxford University Press, New York, 2009).

- 13.109 In the United States, a number of states have actively considered RFID legislation and in a few states, legislation has been passed.¹²³³ The European Commission has adopted a Recommendation that provides guidance on how to operate RFID applications in compliance with privacy and data protection principles and industry has welcomed the framework.¹²³⁴ A central theme is that privacy and information security features should be built into RFID applications before their widespread use.¹²³⁵ The OECD has also issued policy guidance on RFID that covers privacy issues such as transparency and notice, and privacy and security risk assessment.¹²³⁶
- 13.110 In the UK the Information Commissioner has published information about RFID tags and data protection.¹²³⁷ The Office of the Privacy Commissioner of Canada has produced a fact sheet on RFID technology¹²³⁸ and a consultation paper on RFID in the workplace.¹²³⁹ The Information and Privacy Commissioner of Ontario has issued a set of best practice guidelines in collaboration with industry and stakeholders.¹²⁴⁰ As we noted in *Privacy: Concepts and Issues*, an industry code of practice has been developed in New Zealand.¹²⁴¹

BIOMETRICS

- 13.111 In *Privacy: Concepts and Issues*, we discussed certain technologies of the body including biometrics, genetic technology and brain scanning.¹²⁴² Biometric technologies include finger and iris scanning, and facial, voice and gait recognition. They are used to identify individuals or to verify their identity by means of their physical features. Some can be used covertly and at a distance, and in addition to their use in identification they may give clues as to what a person is thinking or feeling.
- 13.112 Biometrics give rise to particular privacy concerns due to their links with a person's bodily identity and sense of personhood. Privacy concerns about the use of biometrics include that the technology makes it easier to monitor people and link information about them and that biometrics may reveal sensitive information such as information about a person's health, emotional state or ethnicity. There are also concerns about security and accuracy.

1233 Julie Manning Magid, Mohan V Tatikonda and Philip L Cochran "Radio Frequency Identification and Privacy Law: An Integrative Approach" (2009) 1 Am Bus LJ 19–22. See also Laura Hildner "Defusing the Threat of RFID: Protecting Consumer Privacy through Technology-Specific Legislation at the State Level" (2006) 41 Harv CR-CL L Rev 133.

1234 Paul Mueller "EC Sets Out Privacy Requirements for Smart RFID Tags" (13 May 2009) *IDG News Service* <http://computerworld.co.nz> (accessed 19 May 2009).

1235 European Commission recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification (12 May 2009) C(2009)3200.

1236 OECD Directorate for Science, Technology and Industry, Organisation for Economic Co-operation and Development *OECD Policy Guidance on Radio Frequency Identification* (Paris, 2008). See Blair Stewart, Assistant Privacy Commissioner "Tracking down good privacy practices for RFID" (Presentation to New Zealand RFID Pathfinder Group, Auckland, 9 July 2009).

1237 Information Commissioner's Office (UK) *Data Protection Technical Guidance – Radio Frequency Identification* (2006) www.ico.gov.uk (accessed 8 December 2009).

1238 Office of the Privacy Commissioner of Canada *RFID Technology* www.privcom.gc.ca (accessed 9 December 2009).

1239 Office of the Privacy Commissioner of Canada *Radio Frequency Identification in the Workplace: Recommendations for Good Practices – a Consultation Paper* (Ottawa, 2008).

1240 Information and Privacy Commissioner of Ontario *Privacy Guidelines for RFID Information Systems* (Toronto, 2006).

1241 GS1 New Zealand *EPC/RFID Consumer Code of Practice* www.gs1nz.org (accessed 18 January 2010); New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) para 6.73.

1242 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) paras 6.90–6.95.

- 13.113 The Irish Council for Bioethics has released a report raising concerns about how personal biometric information is collected and stored and whether there are sufficient controls on who can access it. The Council recommends that any use of biometrics should be proportional to the risk sought to be addressed and that a detailed justification should be provided as to why using biometrics advances the public good. There should be openness and transparency around the use of biometrics. Furthermore, information collected should not be shared without cause, should not be held for longer than necessary, and should be deleted when no longer needed.¹²⁴³
- 13.114 In Australia, the Biometrics Institute developed its own Privacy Code, which was approved by the Australian Privacy Commissioner in 2006 and applies to members of the Institute. The Code modifies the Australian Privacy Act's principles for biometrics, and also adds several supplementary principles, covering protection of biometric information, individuals' ability to control the use of biometric information about them and accountability of members.¹²⁴⁴
- 13.115 The New Zealand Privacy Commissioner has noted that a code of practice is one possible avenue to respond to the issues posed by biometrics, but that this is a resource-intensive option.¹²⁴⁵ The New Zealand Government has released *Guiding Principles for the Use of Biometric Technologies for Government Agencies*.¹²⁴⁶ The new Immigration Act 2009 makes provision for the collection of biometric information by specified immigration officials, and imposes a requirement that the information be dealt with in accordance with the Privacy Act.¹²⁴⁷ Moreover the provisions limit the purposes for which biometric information can be collected.¹²⁴⁸ In respect of the collection and use of biometric information by immigration officials, the Department of Immigration is required to carry out a privacy impact assessment in order to identify the inroads into an individual's privacy, and to consider ways to mitigate any potential harms that are identified.¹²⁴⁹ In doing so, the Department must consult with the Privacy Commissioner.
- 13.116 Noting that agencies are increasingly using biometric information as identifiers, the ALRC has recommended an amendment to the identifier principle (the equivalent of New Zealand's principle 12) to make it clear that the principle covers the use of biometric information for identification purposes.¹²⁵⁰ The Commission recommended that an "identifier" should include "biometric information that is collected for the purpose of automated biometric identification or verification that (a) uniquely identifies or verifies the identity of an individual for the purpose of an agency's operations; or (b) is determined to be an identifier

1243 Irish Council for Bioethics *Biometrics: Enhancing Security or Invading Privacy?* (Dublin, 2009).

1244 Office of the Privacy Commissioner (Cth) "Approval of the Biometrics Institute Privacy Code" (19 July 2006).

1245 Marie Shroff, Privacy Commissioner "Trans Tasman Standardisation for Biometrics" (Address to the Biometrics Institute Trans Tasman Standardisation for Biometrics Conference, Wellington, 1 October 2004).

1246 Cross Government Biometrics Group *Guiding Principles for the Use of Biometric Technologies for Government Agencies* (Wellington, 2009).

1247 Immigration Act 2009, s 31.

1248 Immigration Act 2009, s 30.

1249 Immigration Act 2009, s 32.

1250 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) paras 30.48–30.58, recommendation 30-3. The Australian Law Reform Commission also recommended that biometric information that is collected for the purpose of automated biometric verification or identification, as well as biometric template information, be treated as "sensitive information" for purposes of the Australian Privacy Act: Recommendation 6-4.

by the Privacy Commissioner.”¹²⁵¹ In its response, the Australian Government rejected this information, on the basis that the “identifier” principle is not appropriate for addressing the harm identified by the ALRC.¹²⁵²

PRIVACY- ENHANCING TECHNOLOGIES

13.117 In *Privacy: Concepts and Issues*, we discussed different types of privacy-enhancing technologies (PETs).¹²⁵³ PETs encompass both tools that individuals can use to protect their privacy online (such as encryption and data anonymisation)¹²⁵⁴ and tools that can be used by organisations to minimise the intrusiveness of their systems on the privacy of members of the public. We noted three roles that PETs can play in privacy policy:¹²⁵⁵

- they can compliment other regulatory approaches as part of the privacy protection “toolbox”;
- the use of specified PETs in particular products or services could be mandated by regulation or legislation; or
- they can be used as alternatives to regulation.

We also noted that government can encourage the use of PETs through taking the lead by mandating their adoption by government agencies and other public entities.

13.118 The House of Lords Constitution Committee has recently endorsed the use of PETs to ensure “privacy by design”: that is, ensuring that systems are designed to incorporate privacy protections from the outset.¹²⁵⁶ The committee recommended that the UK Government review its procurement processes so as to incorporate design solutions that include privacy-enhancing technologies in new or planned data gathering and processing systems.¹²⁵⁷ In Canada, the Information and Privacy Commissioner of Ontario has also been very active in promoting “privacy by design”.¹²⁵⁸

13.119 Privacy impact assessments (PIAs) are one tool that could help to identify where PETs could be implemented in the design of new initiatives, and the Privacy Commissioner has produced a *Privacy Impact Assessment Handbook*.¹²⁵⁹ The House of Lords Constitution Committee has recommended that the UK Government amend the provisions of the Data Protection Act 1998 so as to make

1251 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) paras 30.48–30.58 and 30.146, recommendation 30-3.

1252 Australian Government *First Stage Response to the Australian Law Commission Report 108 – For Your Information: Australian Privacy Law and Practice* (Canberra, October 2009) 74.

1253 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 151–156.

1254 See also new developments such as the Vanish programme that makes data unreadable after a certain time period: Mark Harris “How You Can Self-Destruct Your Messages” (16 August 2009) *Times OnLine* <http://technology.timesonline.co.uk> (accessed 20 August 2009); John Markoff “New Technology to Make Digital Data Self-Destruct” (21 July 2009) *The New York Times* www.nytimes.com (accessed 29 July 2009).

1255 Colin J Bennett and Charles D Raab *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press, Cambridge (Mass), 2006) 198–202, cited in New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 155.

1256 House of Lords Constitution Committee *Surveillance: Citizens and the State* (London, 2009).

1257 House of Lords Constitution Committee *Surveillance: Citizens and the State* (London, 2009) para 349.

1258 See, for example, Ann Cavoukian, Information and Privacy Commissioner of Ontario *Privacy by Design: The 7 Foundational Principles* (Toronto, 2009).

1259 Office of the Privacy Commissioner *Privacy Impact Assessment Handbook* (Wellington, 2007).

it mandatory for government departments to produce an independent, publicly available, full and detailed PIA prior to the adoption of any new surveillance, data collection or processing scheme, including new arrangements for data sharing.¹²⁶⁰

- 13.120 The ALRC has recommended that the Privacy Commissioner should have the power to direct a public agency to produce a PIA in relation to a new project or development that the Privacy Commissioner considers may have a significant impact on the handling of personal information.¹²⁶¹ If an agency failed to comply, the Privacy Commissioner would be required to report to the responsible Minister.¹²⁶² The Australian Government accepted this recommendation.¹²⁶³ The ALRC also recommended that the Privacy Commissioner produce guidelines in relation to PIAs,¹²⁶⁴ and that this new function be reviewed in five years' time to assess whether it should be extended to private sector organisations.¹²⁶⁵ This recommendation was also supported by the Australian Government.¹²⁶⁶
- 13.121 The Privacy Commissioner's function to promote an understanding of the privacy principles by education and publicity¹²⁶⁷ is broad enough to enable the Privacy Commissioner to undertake educational programmes about PETs. The ALRC has recommended that in exercising its research and monitoring functions, the Australian Privacy Commissioner's Office should explicitly consider technologies that can be deployed in a privacy-enhancing way; and that the Office should develop and publish education materials for individuals and agencies about specific PETs and privacy-enhancing ways in which technologies can be deployed.¹²⁶⁸ Both recommendations were accepted by the Australian Government in its response.¹²⁶⁹
- 13.122 In the United Kingdom, the Information Commissioner has commissioned research to develop a compelling and understandable business case for investing in proactive privacy protections. This arose from an earlier report that identified the absence of an articulated business case for spending money on privacy-friendly systems as a barrier to more proactive privacy protection.¹²⁷⁰

1260 House of Lords Constitution Committee *Surveillance: Citizens and the State* (London, 2009) para 307. The Information Commissioner, or other independent authorities, should have a role in scrutinising and approving these PIAs.

1261 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) recommendation 47-4(a). The Commission preferred this option to the alternative option of mandatory Privacy Impact Assessments as is the case in Canada: para 47.61.

1262 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) recommendation 47-4(b).

1263 Australian Government *First Stage Response to the Australian Law Commission Report 108 – For Your Information: Australian Privacy Law and Practice* (Canberra, October 2009) 86.

1264 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) recommendation 47-5.

1265 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) rec 47-5.

1266 Australian Government *First Stage Response to the Australian Law Commission Report 108 – For Your Information: Australian Privacy Law and Practice* (Canberra, October 2009) 87.

1267 Privacy Act 1993, s 13(1)(a).

1268 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) recommendations 10-1 and 10-2.

1269 Australian Government *First Stage Response to the Australian Law Commission Report 108 – For Your Information: Australian Privacy Law and Practice* (Canberra, October 2009) 30.

1270 Information Commissioner's Office (UK) *The business case for investing in proactive privacy protection* (London, 2009).

Q158 Do you have any comments about the role of privacy-enhancing technologies in government or the private sector, and how their use could be encouraged?

Q159 Should consideration be given to empowering the Privacy Commissioner to direct public or private sector agencies to produce Privacy Impact Assessments for new projects that may have a significant impact on the handling of personal information?

CONCLUSION

- 13.123 In this chapter we have outlined technological practices that give rise to particular privacy concerns and have asked for views about the issues raised. As noted above, the Privacy Commissioner has a specific function to research and monitor developments in data processing and computer technology, and to ensure that any adverse privacy effects of such developments are minimised.¹²⁷¹ We think that this function should probably be broadened and updated so that instead of referring to “data processing and computer technology” it refers to a broader range of technological developments.¹²⁷² We wonder whether the Privacy Commissioner’s responsibility to *ensure* the minimisation of privacy effects remains realistic and we suggest that this aspect may need to be revisited. We also note that the Australian Privacy Act provides the Australian Privacy Commissioner with an additional function to monitor and report on the adequacy of equipment and user safeguards.¹²⁷³
- 13.124 We invite submissions relating to the functions of the Privacy Commissioner in relation to technological developments, and relating to the topics discussed in this chapter.

Q160 Do you have any comments about the privacy issues associated with the technologies discussed in this chapter? Is any particular law reform or regulatory response required in relation to any or all of these technologies? Should consideration be given to codes of practice or Privacy Commissioner guidelines in relation to any particular technology?

Q161 Do technologies not discussed in this chapter give rise to important privacy issues that require examination?

¹²⁷¹ Privacy Act 1993, s 13(1)(n).

¹²⁷² The Australian Law Reform Commission has recommended deleting the word “computer” from the comparable function of the Australian Privacy Commissioner in the Privacy Act 1988 (Cth), s 27(1)(c): Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) recommendation 47-1.

¹²⁷³ Privacy Act 1988 (Cth), s 27(1)(q).