Paddling in unison or just paddling? International trends in reforming information privacy law

Gehan Gunasekara*

Abstract

The existing paradigms governing the management of personal data globally are under pressure from rapid technological and social change. This article examines recent proposals for modernizing information privacy law in the USA, the European Union, Australia and New Zealand. It finds significant areas of commonality and critically explores points of difference, notably innovations such as the de-coupling of previously linked privacy principles, dichotomies between consumer-facing companies and third parties and new rights such as the right to be forgotten and to erasure, the right to data portability, privacy by design and default and privacy impact assessment. The article argues that the proposals ought to draw on each other’s strengths.

Keywords: information privacy law reform; data protection policy; cross-border personal data transfer

1 Introduction

Personal information is an important currency in the digital age. It can be used to control people, steal their identities or be mined to extract value. Information privacy laws are designed to protect individuals against misuse.

* Associate Professor in Commercial Law, University of Auckland. E-mail: g.gunasekara@auckland.ac.nz.
of their information by corporations and by government. However, in the post-September 11th world, existing paradigms governing information privacy law globally are under threat not only because of government surveillance but also, rather, due to rapid technological and social change. In particular, the evolution of the Internet into web 2.0, the growth of social networking and the convergence of technologies and applications used by individuals has necessitated a global response towards redesigning information privacy laws.

This article examines the response to these challenges by focusing on the specific law reform proposals of four jurisdictions that, for the most part, have yet to be implemented. These are the recommendations of the Australian Law Reform Commission (ALRC), the New Zealand Law Commission (NZLC), the European Union’s Draft Privacy Regulation (EU Draft) and, last but not least, the Consumer Privacy Bill of Rights (CPBR) proposed in 2012 by the Obama Administration in the USA.

Personal information has become a valuable commodity, one which provides the raw material for and underpins the success of corporations such as Google and Facebook. Although a uniform approach in regulating the flow of personal information across jurisdictional borders was needed from an early stage, this imperative is today even more important in an environment of outsourcing and multi-jurisdictional management of personal information. The challenge facing regulators is to ensure they do not stifle innovation and the creation of value from the new technologies. At the same time, however, a new generation of information privacy laws needs to be technologically neutral in order to survive into the future.

The article examines the extent to which the current proposals achieve these twin objectives. It will be seen that the CPBR, ALRC, NZLC and EU Draft all address similar concerns but that their recommendations reflect some philosophical differences as to the way in which individual rights are
balanced against corporate and governmental interests. This article argues for appropriate changes in the core information privacy architecture in order to bridge this divide.

2 International focus of information privacy law

Information privacy law is distinct from, but related to, other branches of privacy law. These include tortious developments in the USA8 and human rights law in Europe. The latter encompasses wider protection of privacy interests under Article 8 of the European Convention on Human Rights9 which contains the right to respect for private and family life but also Articles 8 and 52 of the Charter of Fundamental Rights of the European Union10 which enshrines the right to protection of personal data and specifies that limits on this right must be specified by law, and subject to proportionality and necessity tests.

Information privacy law emerged relatively recently as an outcome of the use of computer and communications technologies and the resulting fear of their use to create a ‘Big Brother’ surveillance society. Early national legislation included the United States Privacy Act of 197411 and the Swedish Data Protection Act 1973.12 Currently, around 100 States have enacted information privacy (or data protection) statutes.13

A natural consequence of these developments was a concern by governments and business that individual jurisdictions’ privacy legislation may impede the free flow of personal data between States with negative socio-economic effects.14 In response, the Organization for Economic Cooperation and Development (OECD) developed a set of principles known as the Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data (OECD Guidelines)15 in 1980.

This seminal instrument16 has influenced not only all subsequent domestic legislation but also later international and regional agreements governing information privacy. Examples of the latter are the European Union’s

11 5 USC section 552 (a) (1988).
16 The Hon Michael Kirby has argued that the non-binding nature of the Guidelines has resulted in their being more successful, at ensuring consistency as to the content of domestic rules, than formal international treaties and agreements. See M Kirby, ‘The History, Achievement and Future of the 1980 OECD Guidelines on Privacy’ (2010) 6 Privacy Law Bulletin 54, 57. For discussion as the role of international agreements concerning
Privacy Directive, the voluntary ‘Safe Harbor’ regime for USA corporations negotiated between the USA and the European Union and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.

Part Two of the OECD Guidelines contains eight basic principles of national application. Broadly, they require organizations and governments that collect personal information to specify why the information is being collected and who it is to be shared with, not to use or share the information otherwise than specified, retain it securely, maintain its accuracy, allow individuals access to their information and to request its correction when necessary. It has been observed that these requirements may be underpinned by a few core principles, such as good faith, transparency and fairness.

Despite such principles-based rules giving uniformity to the substance of most information privacy statutes, the manner of their implementation has varied considerably. The majority of jurisdictions have followed the European lead in enacting over-arching laws spanning their public and private sectors. The USA, however, has preferred to adopt a sectoral approach with specifically tailored legislation for the Government, financial and health sectors to name a few. The latter approach has left gaps in the private sector, which, the CPBR proposes to address.

3 Impetus for reform

Several causes underlie the pressure for reform to existing information privacy paradigms. These include globalization, rapid proliferation of technologies and the social changes wrought as a consequence. The

privacy see Lee Bygrave, ‘International Agreements to Protect Personal Data’ in James Rule and Graham Greenleaf (eds), Global Privacy Protection: The First Generation (Edward Elgar 2008).


19 Available at <http://publications.apec.org> accessed 1 October 2012.

20 They are principles relating to collection limitation, data quality, purpose specification, use limitation, security, openness, individual participation and accountability.


23 Privacy Act 1974, 5 USC section 552; Computer Matching and Privacy Protection Act 1988, 5 USC section 552.


exponential growth of Internet use and applications using it has led to web 2.0 which, in turn, have rendered much of the existing law obsolete.\textsuperscript{27} The current privacy principles are essentially two-dimensional and vertical in nature: they see information flows as principally being between individuals on the one hand and organizations and governments on the other.

With the development of phenomena such as social networking and social media (for example Facebook, Twitter and blogs to name a few) individuals, on the other hand, have become controllers of personal information in their own right. The relationships between them tend to be horizontal and multidimensional, for instance through commenting on each other’s blogs and websites. However, to further compound the difficulties, technologies are now routinely employed whereby individuals interacting with each other also share (often unintentionally) personal information with other organizations. These may be the corporations providing the services allowing individuals to interact with one another as well as third parties such as providers of applications which are supplementary programmes used on social networking services.\textsuperscript{28} Thus, horizontal informational relationships may be supplemented by vertical ones that amount to surveillance.

Encouragingly, the Obama Administration, in its recent policy announcement is cognizant of these dangers:

As third parties become further removed from direct interactions with consumers, it may be more difficult for them to provide consumers with meaningful control over data collection. Data brokers, for example, aggregate personal data from multiple sources, often without interacting with consumers at all.\ldots consumers might not know that these third parties exist.\textsuperscript{29}

The mechanisms proposed for addressing this lacuna will be amongst the issues canvassed below. Others have also been cognizant of the dangers of surveillance posed by the new technologies. In the United Kingdom, the House of Lords Select Committee on the Constitution has described the main features of current surveillance as encompassing pervasiveness, intensity, speed, interconnection and automation, amongst others.\textsuperscript{30} These facilitate practices such as data mining and profiling to occur.\textsuperscript{31}

Furthermore, platforms such as Facebook increasingly provide cloud services allowing the storage and exchange of vast quantities of personal information as well as providing social networking: Facebook’s use by corporations, not for profit groups and individuals has created cross-over

\begin{itemize}
\item Gehan Gunasekara and Alan Toy, “My-Space” or Public Space: The Relevance of Data Protection Laws to Online Social Networking’ (2008) 23 NZULR 191, 193.
\item The White House (n 7) 13.
\item ibid [33].
\end{itemize}
risks when employers and others seek to gain inappropriate access to individuals’ Facebook profiles and private information. The existing information privacy paradigms do not cater well for such third party uses of personal information where it is not the agency holding the individual’s information that shares it with the third party.

Practices undertaken by the providers of the platforms themselves also test the boundaries of individual consent and transparency. For instance Google used information gathered from its Gmail service to set up the Buzz social network which led to an investigation by the United States Federal Trade Commission (FTC) and a settlement in 2011. Settlements were also reached between the FTC and Twitter and the settlement with Facebook allowed that company’s share float to take place in 2012.

It is undoubtedly these events that at least in part prompted the Obama Administration to articulate its policies on privacy with a view to legislative adoption through the CPBR. The announcement marks a watershed for the USA as it represents abandonment of reliance principally on the law prohibiting deceptive and unfair trade practices to rein in corporate privacy breaches.

On the other hand the Obama Administration lays down a challenge to the rest of the world stating that

United States Internet policy has generally avoided fragmented, prescriptive, and unpredictable rules that frustrate innovation and refrained from adopting legal requirements that prescribe specific technical requirements, which could fragment the global market for information technologies and services and inhibit innovation.

The policy statement further states that the USA’s approach has yielded a flexible, voluntary privacy framework that provided meaningful privacy protections while fostering dynamic innovations in technologies and business models.

Clearly, the USA has been the global leader in developing Internet technologies and services. Whatever one’s views as to the implications of this role for personal privacy worldwide, it is obvious that the USA does not intend

---

34 Agreement Containing Consent Order with a service date of 24 June 2011, between Twitter Inc and the Federal Trade Commission (US).
35 Agreement Containing Consent Order with a service date of 10 August 2012, between Facebook Inc and the Federal Trade Commission (US).
37 The White House (n 7) 24.
38 Ibid.
to subscribe to rules that may imperil its role in leading innovation. The information privacy paradigm it has proposed therefore merits study.

One difficulty must be acknowledged at the outset. Unlike the other jurisdictional approaches, that adopted by the CPBR differs somewhat in that it amounts to a statement of broad rights, rather than recommendations for specific rules. Although federal legislation is envisaged, other options feature prominently, such as multi-stakeholder processes using the rights as a template for codes of conduct to be enforced by the FTC. Of necessity, much detail in these codes will have to await elaboration. On the other hand a raft of privacy reports have emanated from the USA in recent years such as the Department of Commerce Report or Green Paper and the more recent FTC Report on Protecting Consumer Privacy (FTC Report). The latter is broadly aligned with the CPBR’s framework but fleshes it out by detailed consideration of topical matters—for instance a ‘do not track’ requirement—and contains key policy settings for future legislation, such as exempting entities that collect data from under 5000 consumers from its requirements.

4 Definitional challenges

Before examining the varied proposals as to the content of the future information privacy law in the next section, it is first important to evaluate the definitional challenges faced by regulators in this area. This is because a crucial threshold issue is whether personal information is caught by the law to begin with.

Central to information privacy laws is the definition of ‘personal information’ or ‘personal data’. The elements of the definition in the EU Directive—for instance that information must ‘relate to’ an individual—have been exhaustively examined by an Article 29 Working Party opinion. The opinion identifies the almost limitless categories of information (such as house values or car service records) that might amount to personal data. Such potential explains in part the narrow interpretation given personal data by some domestic courts for example that ‘The information should have the data subject as its focus rather than some other person with whom he may have been involved or some transaction or event

---

39 ibid 47.
42 Providing it is non-sensitive consumer data that is not shared with third parties; ibid 16.
43 See for example Data Protection Act 1998 (UK), s 1(1).
45 ibid 9-10.
in which he may have figured or had an interest..."46 by contrast, the European Court of Justice has adopted a more expansive approach towards personal data.47

The crux of the matter is that an individual must be ‘identifiable’, or able to be identified, from the information.48 However, the fast moving technological landscape—notably computers and telecommunications—has placed considerable pressure on what can be considered personal information.

For instance so-called ‘Big Data’ is being generated and digitally stored in vast quantities: this includes logs generated by Internet use, call and traffic data from cell phone use as well as location data and logs generated by radio frequency identifier devices (RFID). As a consequence much more information now exists, from which it is theoretically possible to identify someone. One illustration is the question whether Internet Protocol (IP) addresses can amount to identifiable personal information that has been subject to judicial consideration in Europe49 but is likely to be overtaken by other technological issues.

Professor Roth has argued that no limits should be placed on what is ‘personal information’ but that context ought to be the principal guide.50 Another commentator has suggested that information may become personal data relating to and identifying an individual subsequent to its point of collection.51 As will be seen below this view resonates with recent trends in the USA, which see information privacy requirements as flexible ones where outcomes are not necessarily fixed to starting points.

This sensible approach has predominated in the Australian and New Zealand reform proposals where simplicity and technological neutrality have been paramount considerations. In New Zealand the NZLC has recommended the existing definition—‘personal information means information about an identifiable individual’52—not be amended but that the Privacy Commissioner develops guidance from time to time as to what is or is not ‘identifiable’.53 The suggestion would allow flexibility in dealing with new technological applications as they arise. Moreover, the NZLC states that whether or not an IP address is personal information can only be

---

47 Lindqvist v Sweden European Court of Justice C-101/01 (6 November 2003) [24].
49 In a case involving peer to peer file sharing and alleged copyright violation it was held that Internet Protocol addresses were personal data as users could be precisely identified, see Scarlet Extended SA v Societe belge des auteurs, compositeurs et editeurs SCRL (SABAM), European Court of Justice C-70/10 (24 November 2011).
52 Privacy Act 1993 (NZ) s 2(1).
53 Law Commission (NZ) (n 5) R4.
determined in relation to the particular context in which the address is collected, held, used or disclosed.54

Likewise, in Australia, the ARLC has recommended that personal information be defined as information about an individual who is ‘identified or reasonably identifiable’, as opposed to one who is ‘reasonably ascertainable’.55 As with the NZLC recommendation, ongoing guidance by the Privacy Commissioner is proposed as to the meaning of ‘identified’ and ‘reasonably identifiable’.56 On the other hand the addition of a reasonableness element to the definition is significant as it introduces cost implications: consideration as to what is personal information therefore needs to factor in what is practically possible, as opposed to what may be technically possible but unlikely, due to cost. It can be observed that the definition is dependent on the changing context and makes allowance for technological change as what is unlikely today may be feasible in future.

By contrast, the EU Draft’s definition, whilst open-ended, must be seen against the backdrop of a more sophisticated understanding of the interests at stake. For instance an Article 29 Working Party opinion has stated that: ‘The cost… is one factor, but not the only one. The intended purpose, the way the processing is structured, the advantage expected by the controller, the interests at stake for the individuals’ must also be considered.57 The EU Draft defines personal data to mean ‘any information relating to a data subject’58 and data subject in turn is defined to mean:

\[\ldots\text{an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;}(\text{emph} \text{asis added})\].

With the exception of the emphasized words, this differs little from the wording of the existing Directive,60 although the addition of the reasonableness criteria carries the advantages discussed above in relation to the Australian proposals. Reference to online and location data, whilst useful, is susceptible to technological obsolescence.

54 ibid [2.52].
55 Australian Law Reform Commission (n 4) [6.53]; this recommendation has been adopted: see Privacy Amendment (Enhancing Privacy Protection) Act 2012, Schedule 1.
56 ibid Recommendation 6-2.
57 Article 29 Data Protection Working Party (n 44) 15.
58 European Commission (n 6) art 4(2).
59 ibid art 4(1).
60 European Parliament (n 17) art 2(a)—albeit that the Directive in Recital 26 employed the wording ‘means likely reasonably to be used’ in the context of what ‘identifiable’ means.
The USA proposals, encapsulated in the CPBR are similarly open-ended thereby allowing adaptation to new technologies. Personal data is defined to mean:

…any data, including aggregations of data, which is linkable to a specific individual. Personal data may include data that is linked to a specific computer or other device61 (emphasis added).

Commentary in the CPBR suggests that such devices might include identifiers on a smartphone or a family computer used to build up a usage profile.62 Cleary, the use of the crucial term ‘linkable’ is sufficiently technology neutral to permit application to new uses and applications. It is evident then that significant consistency exists in the approaches to defining personal information.

4.1 – Anonymous and aggregated information

Most significant from the definitional standpoint and in terms of the arguments advanced in this article is the FTC Report’s approach towards the contentious issue of personal data that has been made anonymous or aggregated with that of other individuals in a non-identifiable format. Such data is to be excluded by the definition on condition the company commits publicly not to re-identify it and, further, ensures through contractual or other mechanisms that downstream users keep the data in a de-identified form.63 The approach is one of privacy by design as well as linking the definition to other core principles such as transparency and has much to commend it.

5 Resiliency and tension in the information principles

5.1 – Consensus and longevity in principles-based approach

Existing domestic privacy legislation is, for the most part, based on the OECD Guidelines and is therefore remarkably similar in content. Examples include the eight Data Protection Principles in the United Kingdom,64 the 12 Information Privacy Principles in New Zealand65 and the previous 10 National Privacy Principles in Australia.66 Unsurprisingly,
therefore, all the reform proposals addressed in this article are consistent in maintaining the existing principles-based approach with the USA CPBR adopting seven ‘Fair Information Practice Principles’ along similar lines. The FTC Report pares this down further to just three—privacy by design, simplified consumer choice and transparency—but incorporates the substantive requirements of data security, collection limits, retention and accuracy within the privacy by design principle through requiring its adoption throughout an organization at every stage of development of its products and services.67

The antipodean recommendations make few proposals to change the content of the existing privacy principles besides relatively minor technical changes,68 and, in the case of Australia, adopting a set of Uniform Privacy Principles to replace the existing duplication between sectors,69 which has been taken up with the enactment of 13 Australian Privacy Principles (APPs).70 However, an attempt to address one technological challenge in particular proved unsuccessful, as the Australian Government did not accept the Law Commission’s recommendation71 that the identifier principle (which governs the use of unique identifiers and subjects their use to certain safeguards) should apply to biometric information.72

In contrast to these somewhat timid steps the recent northern-hemispheric proposals breathe new life into the development of global information privacy law and would be of potentially momentous import, should they be adopted. Attention is now turned to these measures emanating from the USA and Europe, respectively.

5.2 – CPBR approach: addressing innovation and flexibility

5.2.1 De-coupling the principles

The seven proposed Fair Information Practice Principles contained in the CPBR cover the entire information spectrum from collection, use and storage through to the disclosure and disposal of personal information. To this extent they are unremarkable and follow the familiar architecture of the OECD Guidelines. However, a major feature of the existing paradigm is

67 Federal Trade Commission (n 41) 22.
68 For example, in New Zealand it has been recommended that the collection limitation principle be amended by the addition of a new sub-clause providing that individuals should be able to interact with agencies anonymously or under a pseudonym, where it is lawful and practicable to do so in the circumstances (Law Commission (NZ) (n 5) R35), whereas in Australia an entire new principle, UPP 1, is to the same effect (Australian Law Reform Commission (n 4) [20.71]).
70 Privacy Amendment (Enhancing Privacy Protection) Act 2012, sch 1.
71 Australian Law Reform Commission (n 4) Recommendation 30-3.
the inter-connectedness of the principles. By contrast, the CPBR decouples some of the linked principles.

In the EU, the duty to notify individuals of the purposes of collection and intended uses and recipients of the information is inextricably linked to the duty to conform to the promises thereby made. With relatively few exceptions, personal information may only be processed for purposes compatible with those for which they were collected. Any different purposes must be expressly consented to by the individual concerned. The EU Draft continues this stance.

On the other hand the CPBR’s commentary proposes a major innovation by suggesting that in certain instances the otherwise inter-connected principles may be de-linked. It also proposes a dichotomy between ‘consumer-facing’ companies or ‘first parties’ and ‘third parties’:

... data brokers and other companies that collect personal data without direct consumer interactions or a reasonably detectable presence in consumer-facing activities should seek innovative ways to provide consumers with effective Individual Control. If it is impractical to provide Individual Control, these companies should ensure that they implement other elements of the Consumer Privacy Bill of Rights in ways that adequately protect consumers’ privacy. For example, ... such companies may need to go to extra lengths to implement other principles such as Transparency—by providing clear, public explanations of the roles they play in commercial uses of personal data—as well as providing appropriate use controls once information is collected under the Access and Accuracy and Accountability principles to compensate for the lack of a direct consumer relationship.

It is noteworthy that this approach sees the privacy principles not as hard and fast rules but instead as principles of relative weight that, on occasion, may compete with one another necessitating weighing their relative merits when applied to a specific context. Thus, the CPBR posits that companies that acquire personal information indirectly can still use it for their purposes if they provide enhanced transparency, access, accuracy and accountability. This is important as it addresses increasingly prevalent business practices such as companies that collect personal information from disparate publicly available sources and sell it to customers. The FTC Report recommends that all companies, including such third parties, provide access to the consumer data they hold but that the extent of such access is proportionate to the sensitivity of the data and the nature of its use.

---

73 Exceptions commonly found in most jurisdictions include for historical, statistical or scientific purposes where individuals will not be personally identifiable.
74 European Commission (n 6) art 6 (4).
75 The White House (n 7) 13.
76 Federal Trade Commission (n 41) 71.
The devil may be in the detail, however, as the report suggests excluding some categories such as data used solely for marketing purposes on the one hand,77 as opposed to data held by companies that assemble and evaluate consumer information for use by creditors, employers, insurance companies, landlords and others involved in eligibility decisions affecting consumers, on the other.78 In accordance with the notion of enhanced access and accountability where third parties are concerned, the FTC Report recommends legislation giving access rights to consumers for information held by data brokers and the setting up of a centralized data broker website to which consumer-facing entities provide links.79

Moreover, the CPBR’s Focused Collection principle recognizes that ‘companies may find new uses for personal data after they collect it, provided they take appropriate measures of transparency and individual choice.’ 80 Search engines are cited as an example of socially beneficial Internet services necessitating wide-ranging collection.81 The FTC Report recommends that companies be required to obtain affirmative consent before using consumer data in a materially different manner than when claimed when it was collected as well as where sensitive data is collected.82 Sensitive data is defined somewhat differently to other jurisdictions,83 but differences of this nature are to be expected especially as they are likely to be shaped by the underlying cultural and constitutional norms prevalent in the society.

The recommendations must also be seen against the backdrop of the FTC Report’s opinion as to the circumstances where consumer ‘choice’ is needed and where it is not,84 a fundamental distinction based on the context of the interaction between the business and the consumer which is discussed further in this article in relation to the importance of consent. Apart from sensitive uses, examples given where choice is needed include whether to be tracked across other parties’ websites85 and where material retroactive changes are made to privacy representations such as privacy statements.86 Perhaps more controversially, however, other practices do not require specific choice such as cross-channel marketing87 and data enhancement

---

77 ibid, 65; Whilst at the same time providing consumers with access to a list of consumer data they hold and the ability to suppress its use for marketing.
78 ibid 66.
79 ibid 70.
80 The White House (n 7) 21.
81 ibid.
82 Federal Trade Commission (n 41) 60.
83 Defined to include information about children, financial and health information, social security numbers and precise geolocation data but not, seemingly, religious or political beliefs or sexual orientation; ibid 59.
84 ibid 36–40.
85 ibid 40.
86 ibid 57.
87 That is where a first party uses a variety of channels including the Internet, e-mail, mobile apps and texts, as well as offline methods, to reach the consumer.
involving collecting further personal data about the customer but from third party sources.88

As far as the Fair Information Practice Principles are concerned it is evident that transparency is viewed as a continuing or rolling obligation thereby enabling innovation to occur, one of the fundamental values underpinning the CPBR. In this regard although the Respect for Context principle

\[
\ldots \text{emphasizes the importance of the relationship between a consumer and a company at the time consumers disclose data, it also recognizes that this relationship may change over time in ways not foreseeable at the time of collection. Such adaptive uses of personal data may be the source of innovations that benefit consumers. However, companies must provide appropriate levels of transparency and individual choice—which may be more stringent than was necessary at the time of collection—before reusing personal data}^{89}\ (\text{emphasis added}).
\]

It can be observed that this enables the imperatives of value creation and innovation through use of personal information to be accommodated whilst privacy concerns are assuaged. Although this would preserve the perceived competitive advantage that the USA companies currently enjoy it could be a stumbling-block in the interoperability of privacy laws internationally, unless the compensatory measures put forward in the USA, which are discussed further below, are seen as being ‘adequate’ for maintaining privacy interests.

5.2.2 Delegated lawmaking

A key plank of the CPBR is the development of enforceable Codes of Conduct developed voluntarily through multi-stakeholder processes but underpinned by enforcement by the FTC.90 Once codes are in place, the principal mechanism for compliance will be the tried and tested one of the prohibition of unfair or deceptive acts and practices.91 In this respect the CPBR follows the model established in the USA through the Safe Harbour scheme referred to earlier.92 However, it differs from it in one important respect as the CPBR will now provide a safety net standard for the private sector:

Companies that decline to adopt a code of conduct, or choose not to seek FTC review of a code that they do adopt, would simply be subject to

---

88 Federal Trade Commission (n 41) 42–44.
89 The White House (n 7) 16.
90 The White House (n 7) ch IV.
91 ibid 32.
the general obligations of the legislatively adopted Consumer Privacy Bill of Rights.93

Furthermore, ‘the common baseline of the Consumer Privacy Bill of Rights should help ensure that the codes are consistent’.94 It can be seen that this principled approach once again reflects the view that the overarching principles operate at a higher level of abstraction, allowing more detailed rules to be applied in sector-specific contexts.95 The freedom thereby created for sectors to develop codes to meet their particular needs also caters for the imperatives of flexibility and innovation referred to earlier.

Significantly, the CPBR does not propose to replace existing sector-specific laws that govern the private sector such as those in the financial, health or children’s rights areas.96 Neither is it proposed to regulate privacy outside the purely commercial, consumer-oriented context,97 meaning existing laws and policies governing the Federal Government will remain unaffected. Indeed, the CPBR proposal reflects existing USA information privacy practice. For example, the Financial Services Modernization Act 199998 (also known as the Gramm-Leach-Bliley Act) requires a variety of agencies (including the FTC) to establish ‘appropriate standards for the financial institutions subject to their jurisdiction’ to ‘insure security and confidentiality of customer records and information’ and ‘protect against unauthorized access’ to the records.99 The Children’s Online Privacy Protection Act 1998100 operates a Safe Harbour whereby an operator following self-regulatory guidelines issued by marketing or online industry groups approved by the FTC will be deemed to satisfy the Act’s requirements.101

On the other hand, whilst it is intended to pre-empt the ‘enforcement of State laws against companies that adopt and comply with FTC-approved codes of conduct’,102 gaps will still remain in the USA privacy framework outside the private sector—for example, unlike in Europe, it is unlikely that dissemination of personal information to members of a religious group would fall within the ambit of federal privacy law.103 In the USA, there may well be constitutional constraints that make such a position inevitable. Indeed, the CPBR proclaims a strident note of American exceptionalism:

93 The White House (n 7) 37.
94 ibid 30.
95 Gunasekara and Toy (n 21).
96 See the discussion by Solove, Rotenberg and Schwartz (n 26).
97 The White House (n 7) 36.
98 15 USC Sections 6801-6809.
99 15 USC Section 6801 and see discussion in Solove, Rotenberg and Schwartz (n 26) 714.
100 15 USC Sections 6501-6506.
101 ibid Section 6503; and see discussion in Solove, Rotenberg and Schwartz (n 26) 668.
102 The White House (n 7) 37.
103 Compare this with the celebrated decision of the European Court of Justice in Lindqvist v Aklagarhammaren I Jonhoping (C-101/01) [2003] ECR I – 12971, discussed by Roth (n 27) 538.
United States Constitutional law has long recognized that privacy inter-
ests co-exist alongside fundamental First Amendment rights to freedom
of speech, freedom of the press, and freedom of association. Individuals
and members of the press exercising their free speech rights may
well speak about other individuals and include personal information
in their speech. The Access and Accuracy principle should therefore
be interpreted with full respect for First Amendment values, especially
for non-commercial speakers and individuals exercising freedom of the
press.104

It is therefore likely that these factors will continue to differentiate USA
information privacy law from that of other jurisdictions.105

Co-regulation, through codes of conduct adopted through stakeholder
involvement, is not out of step with trends in the other jurisdictions. The
EU Draft envisages codes of conduct sanctioned by the European
Commission,106 whilst the NZLC proposes continuation of the practice
of binding codes developed by the Privacy Commissioner but requiring
approval by the Governor-General in Council (instead of as present being
issued as deemed regulations) thereby preserving the ability of the
Government of the day to reject a proposed code.107 Despite the ALRC
recommending that codes not be binding,108 the Australian Government
response has been to move Australia closer to the New Zealand approach
through giving the Privacy Commissioner power to request that an organiza-
tion develop a code and impose a mandatory code should it fail to do so.109

The speed and flexibility afforded by codes of practice was demonstrated
recently in New Zealand when the Privacy Commissioner issued an urgent
code110 to cater to the special needs for handling personal information that
arose following the earthquakes that devastated the city of Christchurch in
2010 and 2011.111 A sunset clause was embedded to ensure the Code’s
application was of temporary duration.112

---

104 The White House (n 7) 20.
105 See E Volokh, ‘Freedom of Speech and Information privacy: The Troubling Implications of a Right
to Stop People from Speaking About You’ (2000) 52 Stan LR 1049 and S Singleton, ‘Privacy Versus the
First Amendment: A Skeptical Approach’ (2000) 11 Fordham Intellectual Property, Media and
Entertainment LJ 97.
106 European Commission (n 6) art 38.
107 Law Commission (NZ) (n 5) R 52 & R53.
108 Australian Law Reform Commission (n 4) [48.34].
109 Australian Government (n 72) 89–90; see Privacy Amendment (Enhancing Privacy Protection) Act 2012,
sch 3.
110 Permitted by section 52 of the Privacy Act 1993 (NZ).
112 ibid clause 2; the Code expired on 30 June 2011.
5.3 – EU draft innovations

The EU Draft is in the form of European Union Regulation, and therefore directly applicable in Member States. It is also noteworthy that, under its provisions, it is no longer a general requirement that processing be notified to supervisory authorities, although exceptions remain. However, the draft contains many other innovations that are now addressed.

5.3.1 Right to be forgotten and to erasure

The issue of retention limits for personal information is problematic in the digital era as ease of storage and replication pose formidable obstacles. As has been seen the USA proposals partly address these concerns through enhanced access and correction rights to data held by third parties. On the other hand an alternate approach is to concentrate on the practical incidents of removal of data.

The EU Draft’s proposed new right is aimed at allowing erasure and prevention of further dissemination of personal data especially of personal data relating to a child and applies, *inter alia*, when data are ‘no longer necessary in relation to the purposes for which the data are collected or otherwise processed’. Exceptions include where the data are needed for historical, statistical or research purposes and to comply with a legal obligation. The latter exception is subject to public interest and proportionality requirements. The EU Draft’s proposal is at odds with the approach taken by the other jurisdictions.

For example, the ALRC does not support giving an individual a general right to require that processors destroy personal information they hold about the individual. Instead, a recommendation is made for guidance, by the Privacy Commission, on destruction and rendering personal information non-identifiable. Likewise, the NZLC recommends retaining the existing requirement that personal information not be kept for longer than is required for the purposes for which it may lawfully be used, despite acknowledging Professor Roth’s criticism that this is a ‘weak’ principle.

We have already seen that a cornerstone policy of the CPBR is to enable innovation and new uses for personal information to occur. Accordingly, principle six, governing ‘focused collection’ stipulates that: ‘Companies should securely dispose of or de-identify personal data once they no longer need it, unless they are under a legal obligation to do otherwise’ (Added emphasis). Likewise, the FTC Report calls for retention periods to be ‘flexible and scaled according to the type of relationship and use of the data’.

---

113 See for example the discussion below in regard to cross-border transfers of personal data.
114 European Commission (n 6) art 17(1)(a).
115 ibid art 17(3)(c).
116 ibid art 17(3)(d).
118 Law Commission (NZ) (n 5) [3.55].
giving the example of information pertaining to a lifetime mortgage as opposed to transient online behavioural advertising. These examples relate to where a direct relationship exists between consumers and companies as opposed to information shared with third parties although it is likely the latter will be subject to similar flexible requirements.

By contrast, the EU Draft’s proposal falls into the very trap, of inhibiting innovation, that the CPBR seeks to avoid. For instance, it has been argued European jurisprudence fails to adequately address the need for retention in light of revolutionary new technologies that make new uses for personal information feasible. Even a backdated test—asking if new purposes had they been known at the time of collection would have been justified—is not without difficulty.

The EU Draft, on the other hand, attempts to address one of the incidents of the right to be forgotten and to erasure through requiring a controller that has made personal data public to take ‘all reasonable steps, including technical measures’ to inform third parties processing the data

...that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorized a third party publication of personal data, the controller shall be considered responsible for that publication.

A realistic distinction is thus drawn between the data controller and third parties who have copied or linked to the personal data. However, the criteria for this requirement as well as the principle’s application to specific sectors and situations are relegated to delegated acts to be adopted by the Commission, preserving some flexibility as to its future application. The measures have their USA counterpart in the FTC Report’s support for an ‘eraser button’ through which people can delete content they post online. Just as the EU Draft is sensitive to freedom of expression concerns, the FTC also Report notes that

While consumers should be able to delete much of the information they place on a particular social media site, there may be First Amendment constraints to requiring third parties to delete the same information.

---

120 Ibid 29.
122 European Commission (n 6) art 17 (2).
123 Ibid art 17 (9).
124 Federal Trade Commission (n 41) 70.
125 European Commission (n 6) art 17 (3)(a).
126 Federal Trade Commission (n 41) 71.
5.3.2 Right to data portability

A further innovation introduced by the EU Draft addresses an area related to individual access to personal information.\(^{127}\) Aimed at data held in electronic formats, it encompasses two separate requirements: the right to data in an electronic and structured format allowing further use by the individual,\(^{128}\) as well as the right to transmit the data in the same format.\(^{129}\) It has been observed that the obligation would require organizations such as social media providers and cloud storage providers to allow customers to move their data to competitors offering similar products or services.\(^{130}\)

Leaving aside commercial sensitivities, the question might be asked whether the right to data portability can better be regarded as an incident of the general right to access to personal information itself regarded as one of the fundamental information privacy rights.\(^{131}\) Indeed, rather than being a stand-alone principle, such a right serves to strengthen other principles and enhances their efficiency.

An illustration supporting this view was recently witnessed in New Zealand where an inquiry was concluded into several significant privacy failures by the country’s Accident Compensation Corporation.\(^{132}\) One of the risks highlighted was a systemic failure to separate personal information from that belonging to other individuals, thus making it likely that a response to a request for access to personal information would also contain information pertaining to others.\(^{133}\) The EU Draft’s requirement would focus attention on the manner in which personal information is held and require that it be readily transferable, making it less likely to be held in mixed formats.

The CPBR does not address the issue of data portability as a separate issue but is not entirely insensitive to the difficulties inherent in this arena. Principle five, concerning access and accuracy, stipulates that ‘Consumers have a right to access and correct personal data in usable formats . . . .’ In the digital environment, the right to access one’s data is often in order to be able to change service providers. Arguably, the term ‘usable formats’ is more technologically neutral than the EU Draft’s wording which, despite being applicable to today’s technology, does not anticipate future developments.

\(^{127}\) European Commission (n 6) art 18.

\(^{128}\) ibid art 18(1).

\(^{129}\) ibid 18(2).


\(^{131}\) ‘. . . the right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard’ Appendix to the OECD Guidelines: Explanatory Memorandum (Paris 1980) [58].


\(^{133}\) ibid Recommendation 6.
5.3.3 Profiling

Under this article individuals are not to be subject to measures which produce legal effects on them, based on automated processing, intended to evaluate their behaviour and to make predictions as to their future conduct.134 It would appear the provision encompasses the existing Privacy Directive’s safeguards against automated decisions.135 The proposed new article is clearly aimed at the prevalent practices of data mining and predictive modelling of individual behaviour.

These practices, often developed to combat organized crime and terrorism, have applications elsewhere, particularly in the commercial sphere. In the USA data mining has been described as

the application of database technology and techniques – such as statistical analysis and modelling – to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results.136

The privacy implications of such techniques—notably that analysis of individuals’ personal information results in new secondary information about them—have been examined elsewhere.137 The use of the practice in combating terrorism has been documented,138 but obvious concerns include ‘the accuracy and use of derived personal information, not to mention the individual’s right of access and correction...’.139

Against this backdrop the safeguards proposed by the EU Draft are timely. Exceptions are narrowly framed, including processing associated with contracting by the individual and consent (as will be discussed below) of the individual.140 Significantly, where contracting is invoked there must be transparency as to the intended use for profiling specifically and, crucially, ‘the envisaged effects of such processing on the data subject’.141

It should be noted, however, that the legal requirement can relatively easily be circumvented through use of de-personalized information. For example Facebook states that it

---

134 European Commission (n 6) art 20.
135 European Parliament (n 17) art 15.
137 Gunasekara (n 22) 373.
140 European Commission (n 6) art 20 (2).
141 ibid art 20(4).
may share your information when we have removed from it anything that personally identifies you or combined it with other information so that it no longer personally identifies you.\textsuperscript{142}

The FTC Report’s treatment of anonymous data, discussed above, linking the ability to use such data to transparency and public commitment not to re-identify such data, has some attraction. It has already been observed that the CPBR also stipulates enhanced transparency for non-consumer-facing companies that are likely to undertake data mining and analysis of such data. However, due to the anticipated de-coupling of the principles, it is unlikely that there will be a contractual nexus between the controller and the individual.

The EU Draft also exempts profiling authorized by law, provided there are measures to safeguard the individual’s legitimate interests.\textsuperscript{143} Finally, the EU Draft empowers the Commission to adopt delegated acts to specify more detailed rules as to the measures needed to safeguard the individual’s legitimate interests.\textsuperscript{144}

5.3.4 \textit{Data protection by design and by default}

The EU Draft elevates privacy by design and privacy by default to the status of core obligations.\textsuperscript{145} This represents a significant advance for these concepts that are increasingly seen as vital tools for the protection of privacy. Thus far, they have generally not been regarded as separate legal obligations. An exception is found in the APEC principles that stipulate: ‘personal information protection should be \textit{designed} to prevent the misuse of such information’ within the context of its Preventing Harm principle.\textsuperscript{146} Instead, these concepts have been largely viewed as a means to an end.

From an economic standpoint, the notions of privacy by design and privacy by default are incontrovertible. It makes far better sense to engineer privacy from the outset in the design of systems, technologies and even legislation, than to have to retrofit them later. Privacy impact assessment, discussed below, may be one means to accomplish this. On the other hand, the reduction in the amount of personal information gathered as a consequence of the policy may be an impediment to technological innovation, for the simple reason that discoveries and new uses are often made accidentally from the leftovers from other information processing and uses. It is not clear that the EU Draft’s ‘regard to the state of the art and the cost of implementation’ pays adequate attention to such concerns.

\textsuperscript{142} \textit{https://www.facebook.com/about/privacy/advertising} accessed 1 October 2012.
\textsuperscript{143} European Commission (n 6) art 20(2)(b).
\textsuperscript{144} ibid art 20(5).
\textsuperscript{145} ibid art 23(1) and (2) respectively.
\textsuperscript{146} APEC Privacy Framework [14].
Although the EU Draft contemplates further elaboration on the subject, by the Commission through delegated acts and technical standards, consent is not stated to be an exception to the controller’s obligations arising from the principles of data protection by design and by default. This raises thorny issues: for instance some online social networks, such as LinkedIn, have by their nature default settings that do not permit privacy and have, arguably, a right to set the terms of their membership.

In contrast to the EU Draft, the Australian and New Zealand recommendations pay scant attention to privacy by design and privacy by default as discrete requirements. The ALRC and NZLC recommend education in regard to privacy enhancing technologies (PETs) as well as the convening of expert Privacy by Design panels to promote and raise awareness of them. The ALRC also recommends Privacy Commissioner Guidance on developing technologies and the notifications that may be appropriate when new technologies are used. These are, however, of an entirely different nature to a separate obligation—analogous to a duty of care—to factor such concerns into the design of new products and services.

By contrast, privacy by design is implicit in much of the rhetoric contained in the CPBR and made explicit by the FTC Report. The report distils three principles from the CPBR’s seven: privacy by design, simplified choice and transparency. The design principle incorporates the substantive principles of data security, reasonable collection limits, sound retention practices and data accuracy or, in other words, the familiar gamut of information privacy norms. The advantage of incorporating these as a ‘design’ element is said to be that of ‘baking’ privacy considerations into the product development process. Indeed the FTC Report’s recommendation is that companies should be required to ‘maintain comprehensive data management procedures throughout the life cycle of their products and services’.

The FTC Report also addresses the key requirement of accountability of data controllers by requiring companies to adopt procedural protections to implement the substantive principles. These include measures such as ‘designating personnel responsible for employee privacy training’ and requiring companies to ‘implement accountability mechanisms and conduct regular privacy risk assessments to ensure that privacy issues are addressed throughout an organization’. This recommendation is matched by the EU Draft’s article 22, which details the responsibilities of controllers to

---

147 European Commission (n 6) art 23(3) and (4) respectively.  
148 Australian Law Reform Commission (n 4) Recommendation 10-2 and [10.34].  
149 Law Commission (NZ) (n 5) Recommendation 103.  
151 Federal Trade Commission (n 41) 30.  
152 ibid 32.  
153 ibid 30.  
154 ibid.
demonstrate compliance with their obligations including through adopting internal policies. European doctrine does not regard accountability as a stand-alone principle but, rather, as aimed at ensuring compliance with the other principles and containing two elements: adequate internal measures to ensure compliance and demonstrating externally how this has been accomplished.

5.3.5 Data protection impact assessment

A logical corollary of privacy by design and privacy by default is the technique of conducting privacy impact assessment. In some jurisdictions they are legislatively mandated, especially where government agencies process personal information. The EU Draft elevates this to an autonomous requirement whenever processing is likely to present specific risks to the rights and freedoms of data subjects by virtue of their ‘nature, their scope or their purposes’.

The latter phrase is a useful starting point for discussion. Thus, the wider the nature and scope of the processing, the greater the risks that ought to be considered. On the other hand consideration of the purposes of the processing is problematic. As we have seen, a key difficulty is that technological progress invariably allows new purposes for the use of personal information to arise that were not contemplated at the outset. The CPBR contemplates enhanced transparency in these instances, but would also benefit from the addition of impact assessments.

A good deal has been written about privacy impact assessment and several issues are raised by the subject, most of which are beyond the scope of the present article. It suffices to state that such assessments have economic advantages as well as disadvantages. Managing risks through identifying assets, vulnerabilities and threats may be obvious benefits to be drawn from them but there may be others such as deriving market opportunities and other benefits through engagement with stakeholders—by for instance discovering that customers and other stakeholders place greater or lesser value on some aspects than the organization believed.

Where use of new technologies is concerned one issue is whether the assessment ought to consider impacts on human rights norms other than privacy such as, for example, issues of discrimination associated with use of

---

156 ibid [28].
157 See K Bamberger and D Mulligan, ‘PIA Requirements and privacy Decision-making in US Government Agencies’ in Wright and De Hert (n 121) 225.
158 European Commission (n 6) art 33(1).
159 See D Wright and P De Hert (n 121).
160 W Wright and P De Hert, ‘Introduction to Privacy Impact Assessment’ in Wright and De Hert (n 121) 3, 10–16.
body scanners at airports. Another is whether the assessment applies to legislative measures themselves, although as will be seen this is implicit in the case of the European Union due to its public interest, necessity and proportionality requirements.

Further matters include the extent to which the assessments must be made public and the legal ramifications of the disclosures. One observer has stated:

requiring a legal basis for mandatory impact assessments is one thing, but then using impact assessment as a legal source in disputes or legal interpretation is another thing.

However, this is not something always to be feared. As has been observed elsewhere the principles of information privacy law share many characteristics with the principles of the law of negligence. Indeed, the reasonableness standard runs through many facets of information privacy law. As is the case when considering whether a duty of care in negligence is breached, considerations of cost and benefit must be taken into account and what better way of documenting this than an impact assessment?

The EU Draft provides for both stakeholder input and publicity for the assessment, subject to safeguards. Specific risk scenarios are identified, including sensitive data, automated processing, surveillance and credit reporting. The Commission is empowered to adopt detailed measures for specific contexts. While some flexibility is thereby afforded to respond to emerging technologies a difficulty for privacy impact assessment of a more conceptual nature has been identified by De Hert:

Normally, technology has to be tested out in practice...Can governments and industry be innovative if everything they do has to be preceded by proper, rational and public decision-making? The question is a hard one. Advocating privacy by design and...not allowing trial and error, on the other hand, seem difficult to combine.

Airport security measures are a case in point. Attempts to ensure watertight screening of passengers through scanners and the like in turn tend to spur ever more innovative techniques of evasion by would-be terrorists. De Hert cites the European Union Civil Aviation Security Regulation by way of

---

161 De Hert in Wright and De Hert (n 121) 72.
162 ibid 49.
163 Gunasekara and Toy (n 21) 548.
165 European Commission (n 6) art 33 paras (3)-(5) inclusive.
166 ibid para (2).
167 ibid paras (6) & (7).
168 De Hert in Wright and De Hert (n 121) 48.
illustration, the preamble to which states that it is intended to respond to the need ‘for more flexibility in adopting security measures and procedures in order to meet evolving risk assessments and to allow new technologies to be introduced’.  

Some of the difficulties with privacy impact assessments that have been raised above are dealt with by the EU Draft. For instance, the requirement for publication of the assessment, with safeguards, is included as is the matter of requiring stakeholder input—‘the controller shall seek the views of data subjects or their representatives’—with safeguards. In this area the CPBR contains significant points of commonality with the EU Draft through its anticipated multi-stakeholder mechanisms:

A key goal of the multistakeholder process is to enable stakeholders to modify privacy protections in response to rapid changes in technology, consumer expectations, and market conditions . . .

It is clear that such processes are to be transparent, but it is unclear whether data subjects or their representatives will be included. In principle, the CPBR’s multi-stakeholder mechanism fulfils at least two of the norms for privacy impact assessment, viz, consultation with affected groups and transparency as to the risks and the measures taken to address them. The FTC Report’s ‘privacy by design’ proposals, discussed above, also address many of the concerns underlying the need for privacy impact assessments.

Both stakeholder involvement and disclosure may be more appropriate when privacy impact assessments are conducted by public authorities. They may be more difficult when businesses are involved as the latter may be reluctant to conduct assessments for reasons of commercial sensitivity. Whilst European Union jurisprudence focuses on procedural guarantees against the arbitrary use of personal data and technologies, De Hert suggests that alternative means of compliance ought to apply in the commercial sphere:

Translated to services offered by industry (think about social network sites and search engines), these guarantees need to realize values such as transparency and control by the user . . . It is clear that a right to have technologies assessed before their launch is emerging as a human right . . . involvement and opposition to given facts and choices need

---

170 De Hert in Wright and De Hert (n 121) 49.
171 European Commission (n 6) art 33 (4).
172 The White House (n 7) 27.
to be possible at the beginning, but also later on throughout the process (e.g. when new facts emerge).\textsuperscript{174}

As we have seen this is precisely the route adopted by the CPBR, which sees individual control and transparency as core obligations, as well as being continuous or rolling ones.\textsuperscript{175}

In contrast to these convergent developments in the northern hemisphere the antipodean proposals for privacy impact statements are lacking in substance if not missing entirely. The ALRC recommends giving the Privacy Commissioner power to direct government agencies to conduct privacy impact statements\textsuperscript{176} as well as recommending that there should be guidelines on the subject generally.\textsuperscript{177} The NZLC only contemplates a role for the Privacy Commissioner in relation to information matching (automated processing) by government agencies,\textsuperscript{178} whilst recommending privacy impact assessment be a requirement for all government agencies in general, but that this should be through Cabinet policy rather than through legislation.\textsuperscript{179}

6 The role of consent

The place of consent in information privacy frameworks is problematic. This is because it is variously treated as a basis for processing personal information as well as on occasion an exception to limitations on the use or disclosure of the information. However, there may be an emerging global consensus as to its proper role. The Australasian recommendations, for example, state that consent ought not to be seen as a separate principle. Indeed, the ALRC points to architectural reasons for such a stance:

\begin{quote}
It would be inappropriate to deal with consent as a discrete privacy principle. The concept of consent is built into the architecture of those principles to which it is relevant. Such an approach emphasizes that consent may have a role to play in various parts of the information cycle.\textsuperscript{180}
\end{quote}

In pointing to the reality that consent is only one of several exceptions or bases for processing personal information, the ALRC is at pains to deny that it should be the ‘overriding factor in permitting or restricting the handling of personal information’.\textsuperscript{181}

\begin{footnotes}
\footnotetext[174]{De Hert in Wright and De Hert (n 121) 75.}
\footnotetext[175]{Individual control (Principle 1) & Transparency (Principle 2).}
\footnotetext[176]{Australian Law Reform Commission (n 4) Recommendation 47-4.}
\footnotetext[177]{Ibid Recommendation 47-5.}
\footnotetext[178]{Law Commission (NZ) (n 5) R 131.}
\footnotetext[179]{Ibid R104.}
\footnotetext[180]{Australian Law Reform Commission (n 4) [19.75].}
\footnotetext[181]{Ibid, [19.76].}
\end{footnotes}
The EU Draft usefully articulates the meaning of consent where it applies. In the first place, the burden of proving consent is shifted to the controller. Importantly, the article also prohibits ‘bundled’ consents whereby consent to allow the processing of personal information is tied to general terms and conditions. Likewise, the FTC Report stresses that companies should provide choices at a time and in a context in which the consumer is making a decision about his or her data, and outside of a privacy policy or other legal document when necessary. Consent and transparency are inextricably linked. The EU Draft would bring the law into line with privacy best practice. For example, layered privacy statements are regarded as preferable to lengthy ones.

The EU Draft expressly provides that individuals retain the right to withdraw consent to the processing of their information at any time. In this respect, there is significant commonality between the EU Draft and the CPBR as the latter states that: ‘Companies should offer consumers means to withdraw or limit consent that are as accessible and easily used as the methods for granting consent in the first place.’ This co-incidentally adopts the core principle of proportionality. On the other hand the USA proposals do not appear to contemplate the right to withdraw consent to processing undertaken by non-consumer facing companies or third parties as outlined above.

The more critical treatment of consent is timely. Professor Solove observes that

Some privacy problems shape behaviour. People often surrender personal data to companies because they perceive that they do not have much choice. They might also do so because they lack knowledge about the potential future uses of the information. Part of the privacy problem in these cases involves people’s limited bargaining power respecting privacy and inability to assess the privacy risks.

The CPBR’s reliance on the ability of individuals to make ‘meaningful decisions’ is elaborated upon, as to where consumer choice is needed, by the FTC Report. The proposed test focuses on the context of the interaction between the business and the consumer and, as we have seen, differentiates

---

182 European Commission (n 6) art 7.
183 Ibid para 1.
184 Ibid para 2.
185 Federal Trade Commission (n 41) 48.
186 Ibid, 27.
188 European Commission (n 6) art 7, para 3.
189 Individual Control principle.
190 See Gunasekara and Toy (n 21) 543.
192 Individual Control principle.
between first parties and third parties that handle personal data. Where first parties are concerned, it stipulates they do not need to provide choice before collecting and using consumer data for practices consistent with the context of the transaction or the company’s relationship with the consumer.193

On the other hand, the FTC Report contemplates ‘affirmative express consent’ as needed whenever companies use consumer data in a materially different manner than claimed when it was collected or when collecting sensitive data.194 Crucially, the sharing of personal data with third parties does not require specific choice, being left to the separate transparency principle. The report does, however, share common ground with the EU Draft as it addresses the issue of ‘take it or leave it’ choices provided by companies for important products or services. Such a choice when collecting consumers’ information, in a manner inconsistent with the context of the interaction between the business and the consumer, would not be a meaningful one.195 Examples given include patented medical devices with few substitutes and even access to broadband Internet access:

\[
\ldots\text{the service provider should not condition the provision of broadband on the customer’s agreeing to, for example, allow the service provider to track all of the customer’s online activity for marketing purposes. Consumers’ privacy interests ought not to be put at risk in such one-sided transactions.}\]

At the other end, the FTC Report regards take it or leave it choice as acceptable for less important products and services in markets with sufficient alternatives, provided ‘the terms of the exchange are transparent and fairly disclosed’.197 Such an economic analysis is consistent with the approach taken by European data protection experts towards similar dilemmas. For example, the Article 29 Working Party has referred to economic incentives for individuals to participate in electronic health record systems where ‘consent is not sufficiently free’.198

On the other hand European data protection requirements relating to consent are far more sophisticated than are suggested by such simple parallels. The Article 29 Working Party has stated that ‘consent is related to the concept of informational self-determination’ and ‘does not waive the application of other principles’.199 These principles, replicated in the EU Draft concern:

\[
\ldots\text{fairness, necessity and proportionality, as well as data quality. For instance, even if the processing...is based on the consent of the user,}\]

---
194 ibid 60.
195 ibid 51–52.
196 ibid 52.
197 ibid.
199 ibid 7–9.
this would not legitimise the collection of data which is excessive in relation to a particular purpose.\footnote{ibid; see European Commission (n 6) art 6.}

The EU Draft’s new stipulations on consent must, therefore, be read in conjunction with Article 6 (which stipulates conditions for the lawfulness of processing), Article 8 (which deals with processing of personal data of a child) and Article 82 that deals with processing in connection with employment. The conditions in Article 6 include processing associated with a contract to which the individual is a party, or intends to enter,\footnote{European Commission (n 6) art 6 (1)(b).} compliance with legal obligations,\footnote{ibid art 6 (1)(c).} protection of the data subject’s vital interests,\footnote{ibid art 6 (1)(d).} and processing necessary to pursue the legitimate interests of the controller provided they do not override the privacy rights of the data subject.\footnote{ibid art 6 (1)(f).} Commentators have observed that European Union jurisprudence on legitimate purposes is ‘very government and industry friendly’.\footnote{Paul De Hert, ‘A Human Rights Perspective on Privacy and Data Protection Impact Assessments’ in D Wright and P De Hert (eds), Privacy Impact Assessment (Springer 2012) 33, 50.}

It may be that these conditions are broadly analogous to the USA proposals which, as outlined earlier, permit the use of consumer data for practices that are consistent with the context of the transaction in question or the company’s existing relationship with the consumer. The USA proposals relating to ‘privacy by design’, encapsulating collection limitation, data quality and security principles together with the transparency requirements such as enhanced access to personal data held by third parties and the like, represent the other two legs of the three-legged privacy framework proposed by the FTC Report. These limbs operate independently of the requirements relating to ‘consumer choice’ and are thus comparable with European understanding as to the operation of data protection norms.

The EU Draft however stipulates that consent is not to be a legal basis for processing personal information ‘where there is a significant imbalance in the form of dependence between the position of the data subject and the controller’.\footnote{European Commission (n 6) art 7, para 4.} This draws upon broader European jurisprudence such as that emanating from the employment sphere.\footnote{Article 29 Data Protection Working Party Opinion 15/2011 (n 199) 7 and see Judgment of the Court (Grand Chamber) of 5 October 2004, Pfeiffer, Roith, Süß, Winter, Nestvogel, Zeller, Diöbele in joined Cases C-397/01 to C-403/01.}

The performance of tasks in the public interest or the exercise of official authority by public authorities is subject to further safeguards.\footnote{European Commission (n 6) art 6(3).} This must be authorized by law and is subject to public interest and proportionality tests.\footnote{ibid.} Compliance with legal obligations is also subject to the same criteria.
There are no equivalents in the CPBR, which, as we have seen, is only intended to apply to the private sector. As far as compliance with legal obligations is concerned, this exception runs through many of the Fair Information Practice Principles and it is clear that where collection is concerned, the CPBR views consent as being inferred for law enforcement and other legal obligations.\textsuperscript{210} Likewise, the FTC Report states unequivocally that ‘Companies do not need to provide choice before collecting and using consumer data for practices that are ... required or specifically authorised by law.’\textsuperscript{211}

It can be observed, as a consequence, that although considerable similarities exist in the role assigned consent in the proposed information privacy landscape in the USA and Europe, significant differences are also found where the processing of personal information takes place pursuant to legal requirements or for non-commercial purposes. In this respect, however, the EU Draft stands apart as in New Zealand, for example, the NZLC follows essentially the USA approach by recommending that in case of inconsistency between a privacy principle and another Act, the other Act will prevail.\textsuperscript{212}

The Australian and New Zealand reform proposals do not specifically address the place of consent beyond what has already been mentioned above. Many of the requirements of the existing principles in New Zealand may be avoided by an agency where the individual concerned ‘authorises’ the departure;\textsuperscript{213} whilst the new APPs contain the concept of an individual ‘consenting’ to a departure from their requirements.\textsuperscript{214} The more insightful treatment of consent by the USA and European proposals is therefore welcome.

7 Data breach notification

An area in which significant consensus has emerged internationally is the need for notification to information subjects or data protection authorities when personal information is lost or inappropriately accessed (accidentally or otherwise). The ability of hackers to utilize fast-changing technologies to hack into databases, as well as the ability of technology to store and transmit ever-increasing quantities of personal information—for example through portable storage devices and through e-mail and cloud services—has meant that the OECD Guideline’s ‘reasonable security safeguards’ principle has proved insufficient, on its own, to deal with the threat.

\textsuperscript{210} The White House (n 7) 17.
\textsuperscript{211} Federal Trade Commission (n 41) 48.
\textsuperscript{212} Law Commission (NZ) (n 5) R 80.
\textsuperscript{213} For example see Privacy Act 1993, s 6 Information Privacy Principle 11 (d).
\textsuperscript{214} Privacy Amendment (Enhancing Privacy Protection) Act 2012, Schedule 1, Australian Privacy Principle 6.1 (a).
Discussion of the different jurisdictional approaches in tackling this issue is beyond the scope of the present article except to note they are broadly in alignment whilst differing in matters of detail. The CPBR for instance recommends replacing the various existing state laws in the USA and pre-empting future state legislation through the creation of a national standard for notifying consumers in the event of unauthorized disclosures of certain types of personal data. The national standard would mean notification is mandatory except when there is no reasonable risk of harm or fraud taking place as a result of the breach.

The EU Draft as well as the Australian and New Zealand reform proposals also recommend mandatory breach notification. The ALRC recommends the creation of an entirely new obligation to notify the Privacy Commissioner and affected individuals where there is a ‘real risk of serious harm’, although this has yet to be enacted. The NZLC, on the other hand, recommends that data breach be incorporated as a component of the existing security safeguards principle, with elaboration as to detail stipulated in the legislation’s mechanical provisions, alongside other provisions governing the manner in which individuals may access their personal information and the grounds upon which access may be denied.

The proposals for reforming the law relating to data breach notification have much in common such as in relation to thresholds for disclosure, exceptions, mechanics and procedure. Comparison of these is beyond the confines of the present article.

8 International interoperability

The facet of information privacy law that causes the greatest difficulty in theory and application is the regulation of personal information flows across borders. This was the original impetus for the development of the OECD Guidelines and has continued to bedevil regulators. Technology has of course in the meantime moved apace. For example, two privacy consultants, Malcolm Crompton and Peter Ford, are cited by the ALRC as saying that

---

215 The White House (n 7) 39.
217 European Commission (n 6) arts 31 and 32.
218 Australian Law Commission (n 4) Recommendation 51-1.
219 Law Commission (NZ) (n 5) R 76 and [7.33]; an advantage with this approach is that New Zealand already possesses an established jurisprudence stemming from its freedom of information legislation of the 1980’s which may be drawn upon by way of analogy, see generally I Eagles, M Taggart and G Liddell, Freedom of Information in New Zealand (OUP 1992).
220 Gunasekara (n 22).
221 Australian Law Reform Commission (n 4) [31.38].
It is no longer accurate to describe data as ‘flowing’ at all...Instead of point to point transfers, information is now commonly distributed among a number of data centres and is accessible globally over the Internet or over private networks.222

In essence, however, the solutions have tended to gravitate towards two or three models, all of which have variously been employed to differing extents by most jurisdictions.

The approach adopted by the European Union has been that of data export control—prohibition of transfer with certain exceptions.223 Another possibility is accountability—either strict or subject to a negligence standard—meaning vicarious liability of the transferor for the actions of subsequent transferees. Finally, a hybrid is possible between these models.

However, in order to achieve consistency in developing a framework for information privacy law that maximizes the potential for innovation whilst protecting individual privacy, variances and nuances within these paradigms need to be safely navigated. The CPBR outlines the challenge in these terms:

globally distributed architecture helps deliver cost-effective, innovative new services to consumers, companies, and governments. It also allows consumers and companies to send the personal data they generate and use to recipients all over the world. Consumer data privacy frameworks should not only facilitate these technologies and business models but also adapt rapidly to those that have yet to emerge.

Though governments may take different approaches to meeting these challenges, it is critical to the continued growth of the digital economy that they strive to create interoperability between privacy regimes.224

The CPBR proposes three strategies in order to meet these goals:

- mutual recognition;
- developing codes of conduct through multi-stakeholder processes; and
- enforcement cooperation.225

All of these have their counterpart to some extent in the recommendations stemming from the other jurisdictions.

---

223 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data chapter IV.
224 The White House (n 7) 31.
225 ibid 31.
Mutual recognition, for its part, is said to be underpinned by two principles: effective enforcement and the ability to demonstrate accountability.\textsuperscript{226} These concepts are clearly interlinked. The USA reliance on the FTC’s case by case enforcement of the prohibitions on unfair or deceptive acts and practices is said by the CPBR to foster ‘evolving standards for handling personal data in the private sector’.\textsuperscript{227} That may be so but the intended promulgation of the Fair Information Practice Principles clearly signifies a shift in approach from relying on this method of enforcement alone.\textsuperscript{228}

Demonstrating accountability is a different problem. As discussed above the notion of accountability is seen as containing an internal and external dimension. The CPBR refers to the voluntary system of Cross Border Privacy Rules, based on the privacy principles contained in the APEC Privacy Framework, that APEC member economies have agreed to recognize.\textsuperscript{229} Such rules, including binding corporate rules adopted by companies, bring the two aspects of accountability together but are not without difficulty as shortcomings in the internal measures are conceptually distinct from the failure to adhere to the publicly notified rules.\textsuperscript{230} Likewise, the Safe Harbour Frameworks that the USA has negotiated with the European Union and Switzerland are seen as mechanisms for recognition.\textsuperscript{231} Self-certification and verification are other options,\textsuperscript{232} and implicit in this are privacy seal\textsuperscript{233} and Trustmark schemes.\textsuperscript{234}

The second strategy outlined by the CPBR is the adoption of codes of conduct through multi-stakeholder processes at the international level akin to those adopted domestically within the USA.\textsuperscript{235} The nature of devolved regulation anticipated by such processes has already been outlined earlier in this article. Disappointingly, the CPBR contemplates that these processes will lead to a ‘transatlantic consensus on important, emerging privacy issues’\textsuperscript{236}, ignoring the potential input of other nations.

The third strategy relating to enforcement cooperation holds much promise as all the other jurisdictions give due prominence to it. This includes sharing of information between enforcement agencies and, eventually, a

\begin{itemize}
\item \textsuperscript{226} ibid 31.
\item \textsuperscript{227} ibid 32.
\item \textsuperscript{228} The approach may be criticized as one leading to perverse incentives whereby non-disclosure of privacy practices will diminish the risk of liability for deceptive practices.
\item \textsuperscript{229} The White House (n 7) 32.
\item \textsuperscript{230} For instance, ought there to be a duty on entities to update internal procedures for implementation each time new technologies with privacy implications are introduced?
\item \textsuperscript{231} The White House (n 7) 32.
\item \textsuperscript{232} ibid.
\item \textsuperscript{233} Such as BBB online <http://www.bbb.org/us/bbb-online-business/?company> accessed 1 October 2012.
\item \textsuperscript{234} See TRUSTe <http://www.truste.com/> accessed 1 October 2012.
\item \textsuperscript{235} The White House (n 7) 33.
\item \textsuperscript{236} ibid.
\end{itemize}
referral system for complaints. Some moves in this direction have already been embarked upon through using the Internet itself as an enforcement tool, through the Global Privacy Enforcement Network (GPEN). All the jurisdictions discussed in this article already belong to this network that is still embryonic in nature.

By contrast, the EU Draft retains the data export control model. Similarly, the Commission is empowered to make adequacy decisions with respect to the level of personal data protection conferred by the jurisdictions to which it is intended to send personal data. In other circumstances, personal data may be transferred outside the European Union provided ‘appropriate safeguards’ exist: these include binding corporate rules, standard data protection clauses adopted by the European Commission or by a domestic supervisory authority and contractual clauses authorized by the latter.

Other derogations from the rule against exports are the requirements for consent of the data subject, processing associated with a contract to which the individual is or intends to be a party, protection of the data subject’s vital interests, transfer in the public interest, transfer connected with legal claims, transfer from a public register and the need to pursue the legitimate interests of the controller or processor. Where the latter ground is invoked there is an enhanced transparency requirement to document the safeguards taken as well as a requirement to inform the supervisory authority—an exception to the general rule that notification is not required.

The EU Draft specifically contains measures stipulating the requirements for binding corporate rules approved by supervisory authorities. In essence, this is an extension of the law of agency or deemed agency that already exists in many other applications, for example the power of company directors to bind their company, and the power of partners to bind their firm. It differs from vicarious liability because the liability is a strict one: provided the breach was by a member of the corporate group the obligation may be enforced against any other member of the group unless the first mentioned member was not itself in breach. Finally, the EU Draft foresees both codes of conduct and certification through data protection seals and marks, although the detail is left to delegated acts by the Commission.
Meanwhile the Australian and New Zealand recommendations on cross-border data flows, for their part, contain surprising discrepancies in their approaches. In Australia, the ALRC recommendation, for a new principle regulating cross-border data flows, has been adopted.\(^{250}\) This holds the transferor accountable for the transferred information and its use by the recipient unless the transferor is able to adduce a reasonable belief that the information would be protected by measures—contractual or otherwise—that are ‘substantially similar’ to the protection afforded by the Australian regime.\(^{251}\) This amounts to a negligence, rather than strict liability, standard.

Exceptions include individual consent and disclosure pursuant to legal requirements\(^{252}\)—these differ from the more stringent approaches to such matters adopted by the EU Draft discussed above. It is also noteworthy that the ALRC dismisses the use of trust marks as a mechanism for recognition as ‘premature’.\(^{253}\)

The approach in New Zealand, on the other hand, is a hybrid between the accountability and data export models. In the first place, the NZLC proposes that transferors must take ‘reasonable’ steps to ensure that ‘acceptable’ privacy standards will apply to the information.\(^{254}\) Exceptions are tightly drawn and include only disclosures to the individual concerned (an obvious but necessary exemption), for maintenance of the law and the avoidance of serious threats to public health or safety—the two latter exceptions being subject to a necessity test.\(^{255}\)

Further, the recommendations propose giving the Privacy Commissioner power to approve ‘specified overseas privacy frameworks’ as providing acceptable privacy standards,\(^{256}\) as well as recommending that the Privacy Commissioner furnish guidance—similar to that proposed in Australia—to agencies when conducting due diligence on transfer.\(^{257}\) Thus, it will be seen that New Zealand will be somewhat closer to the European Union in some respects as the Privacy Commissioner-approved frameworks resemble a Safe Harbour. The New Zealand recommendations differ from those of Australia in another aspect, viz., articulating a strict liability criterion for domestic outsourcing.\(^{258}\)

\(^{250}\) Australian Law Commission (n 4) UPP 11; Recommendation 31-8 and [31]; Privacy Amendment (Enhancing Privacy Protection) Act 2012. Schedule 1 Australian Privacy Principle 8.

\(^{251}\) Privacy Amendment (Enhancing Privacy Protection) Act 2012. Schedule 1 Australian Privacy Principle 8.2.

\(^{252}\) ibid.

\(^{253}\) ibid R110.

\(^{254}\) ibid R111.

\(^{255}\) ibid R112.

\(^{256}\) ibid R113.

\(^{257}\) ibid R107: ‘An agency is responsible for personal information it holds, including information that has been transferred to a third party for storage, custody or processing’.

\(^{258}\) ibid R107.
Finally, all the jurisdictions address the issue of cross-border enforcement of privacy laws, in addition to the guidance emanating from the OECD. The USA regards this, as outlined above, as one of the three central pillars in its approach. The EU Draft empowers the Commission and supervisory authorities to take appropriate steps to facilitate cooperation in enforcement. The NZLC recommends legislation specifically providing for information sharing, assistance and mutual cooperation with overseas privacy authorities as well as enhancing the existing specialist tribunals’ powers in this area. For its part the ALRC does not see any additional measures as needed but catalogues existing agreements and schemes that operate in Australia in this sphere.

9 Conclusions

The governance of personal information has become a matter of increased importance globally. This is attributable at least in part to the pressures of globalization, the spread of technology and the Internet. This article has examined the response to these challenges by four jurisdictions that have proposed modernizing their information privacy regimes to cater to the needs of this century.

Despite information privacy law worldwide employing a common language and adopting, from inception, a presumed technology-neutral paradigm that was remarkably prescient, the exponential social and technological changes witnessed in the last few decades has necessitated a re-think of the existing principles-based rules. This re-evaluation has resulted in a surprising degree of commonality in the proposed jurisdictional solutions. These include adopting technologically neutral definitions of personal information, privacy by design, accountability (as a mechanism for implementation and mutual recognition) and privacy impact assessments. In all these areas the European Union and the USA have been well ahead of the antipodean nations.

Furthermore, an innovation of considerable significance is the USA proposal to re-formulate existing privacy principles in a more fluid configuration in order to facilitate innovation through new uses of information. The dichotomy between consumer-facing companies and third parties with differing obligations attached to each is novel. It has been said that ‘US corporations are the world’s leading commercial exploiters of personal data’ and ‘have been able to use their economic and political

---

260 European Commission (n 6) art 45.
261 Law Commission (NZ) (n 5) R114.
262 Australian Law Commission (n 4) [31.219]-[31.222].
power to use personal data how they wish until now.\textsuperscript{263} That may be about to change.

The attractiveness of the USA proposals for reform is that they would enable many current business practices there, such as data brokerage, to continue whilst gradually bringing individual privacy rights into alignment with those provided by other jurisdictions as the enhanced access rights to data held by third parties and transparency mechanisms take hold. There are differences of detail, such as where direct marketing by consumer-facing companies is concerned, or understanding as to what constitutes ‘sensitive’ information, but these are fairly minor when compared to the advantages to be gained from a common acceptance of the broad information privacy paradigm.

Another feature apparent within the jurisdictional approaches is that both centripetal and centrifugal forces are at work. The USA tends towards the latter by delegating responsibility for detailed lawmaking to the players themselves together with strong centralized enforcement, whereas the European Union proposals would retain responsibility at the centre by leaving much of the detail to be clarified through subsequent elaboration by the European Commission. These distinctions will have a bearing on the ability of the law to be flexible and to respond rapidly to future developments.

Should the USA follow through with its proposals, it would have moved significantly towards accepting the stance of the other jurisdictions, thereby considerably facilitating global trade and commerce. The argument advanced in this article has been that it may be necessary for the other jurisdictions to modify their own information privacy architecture in the direction signalled by the USA in order to accommodate a global convergence. The resulting regime would be more future-proof and friendly to technological innovation. The jurisdictional proposals examined above all share a common language (with some differences as to translation!) but all are generally paddling in the same direction, although the northern hemispheric nations are somewhat ahead of the antipodean ones.

\textsuperscript{263} Greenleaf (n 13) 24.