Improving the Communication of Privacy Information for Consumers

UTS
UNIVERSITY OF TECHNOLOGY SYDNEY

accan

Improving the Communication of Privacy Information for Consumers

Issues, Options and Recommendations

Mark Briedis, Jane Webb and Michael Fraser
February 2016

Improving the Communication of Privacy Information for Consumers

Authored by **Mark Briedis, Jane Webb and Michael Fraser**

Published in **2016**

The operation of the Australian Communications Consumer Action Network is made possible by funding provided by the Commonwealth of Australia under section 593 of the *Telecommunications Act 1997*. This funding is recovered from charges on telecommunications carriers.

University of Technology Sydney – Communications Law Centre
Website: http://www.uts.edu.au/
Email: clc.admin@uts.edu.au
Telephone: **+61 2 9514 9936**

Australian Communications Consumer Action Network
Website: www.accan.org.au
Email: grants@accan.org.au
Telephone: 02 9288 4000
TTY: 02 9281 5322

ISBN: 978-1-921974-38-0
Cover image: Shutterstock 2016

This work can be cited as: Briedis, M., Webb, J. & Fraser, M. (2016). *Improving the Communication of Privacy Information for Consumers*, Australian Communications Consumer Action Network, Sydney.

Acknowledgements

The Communications Law Centre, University of Technology Sydney, would like to thank the members of the Industry and Regulatory Reference Group for taking the time to meet and discuss the issues raised in this research and for providing feedback on the report:

Samantha Yorke, Google

Jeannette Scott, Association of Data-driven Marketing and Advertising

Daad Soufi, Interactive Advertising Bureau Australia

Annan Boag, Office of the Australian Information Commissioner

Scott Gregson, Australian Competition and Consumer Commission

1. Executive Summary

Few people would be surprised to learn that privacy policies and online contracts are rarely read. This point was humorously brought to public attention when UK company GameStation included a clause giving them an unlimited, non-transferrable right to consumers' souls – to which 7500 consumers signalled their consent.[1] The terms of service were an April Fool's joke, but it made an important point – people tend not to read terms and conditions when shopping online, and companies are not challenged on what they include in these documents.

It would be easy to conclude from this example that consumers do not care about their privacy. Evidence points to the contrary. Seventy-nine per cent of Australians have indicated that they do not like their personal information being sent offshore; 78 per cent are uncomfortable with their activities being monitored online; 77 per cent dislike having information about them being stored in order to receive targeted offers; and 60 per cent have decided not to deal with an organisation because of privacy concerns.[2]

It seems likely therefore that the failure of consumers to read privacy communications is not due to a lack of interest in privacy, but to how information about privacy is communicated. This report seeks to canvas all issues important to the communication of privacy information to consumers in order to build a strategic platform for future research and policy work.

One of the goals of future research should be to build a robust body of empirical knowledge about how consumers make decisions in different digital environments and platforms based upon the way in which information about privacy is communicated. This knowledge could then be used to create and test models for better privacy communications and improved levels of consumer empowerment.

Alongside the question of communication exists the question of law. This report considers relevant consumer and privacy law and the extent to which it provides consumers with adequate protection of their personal information. Improving the communication of privacy information to consumers should be accompanied by improvements in the ability of consumers to provide informed consent for the use of their personal information and to exercise a higher level of control over how their personal information is used.

This project conceives of the communication of privacy information in broad terms – it encompasses the entire scope of communication that a business has with its customers. At the most obvious level, the communication of privacy information concerns the problem of how to ensure that consumers read and engage with privacy policies, privacy notices and other materials intended to inform the consumer about a service provider's practices in handling personal information.

However, the communication problem is deeper because it relates to practices, business models and technologies that are complex and in a state of flux. In order for consumers to understand many of

[1] Shoppers unknowingly sold souls - http://fxn.ws/1Ja9jH3

[2] Office of the Australian Information Commission (OAIC) report, Community Attitudes to Privacy survey (2013), pp3-6

the practices described in privacy policies, they would need to have a good, if not expert, knowledge of the practices that privacy policies describe.

A lack of knowledge on the part of some consumers undermines their ability to provide informed consent for the collection and use of their personal information. It may also lead consumers to feel uncomfortable with practices they have a poor understanding of, undermining consumers' trust and confidence in service providers.

Communication with consumers also relates to consumers' basic understanding of the legal purpose of privacy communications and contractual terms that are intended to bind them. Empowering consumers to exercise an adequate level of control over how their personal information is handled should begin with consumers understanding the legal nature of the relationship that privacy communications seek to establish.

Legal and policy issues

Privacy communications do not currently serve consumers well. They tend to be legalistic and technical, rather than helpful and informative. This not only affects the ability of service providers to provide clear information to consumers, but also the ability of consumers to take steps as legal actors, for example by giving or withholding consent for the collection and use of personal information. This research, therefore, concerns itself both with communications and legal issues. With respect to legal issues, contracts that state that consumers provide acceptance through use of a service ('browsewrap') or by clicking a button ('clickwrap') seem likely to be open to legal challenge on the basis that acceptance provided in these circumstances is not valid.

While the validity and fairness of many consumer contracts appear to be open to legal challenge, and it is possible that law reform may encourage improvements in the provision of consent, there is an opportunity for service providers to innovate and compete in providing consumers with better information about privacy and more opportunities for informed consent.

Currently, the Privacy Act only requires consent for the collection of *sensitive* personal information.[3] However, consumers have an interest in all personal information collected online, not just sensitive information, due to the capability of information holders to aggregate information, to analyse it in order to create rich profiles of individuals, and to link anonymous information to identifiable information.

Where service providers request consent, the question of whether it has been legitimately provided should be determined by the extent to which it is adequately informed, provided voluntarily, whether it is current and specific, and whether the individual has the capacity to understand and communicate their consent.[4]

At the most basic level, information provided to consumers should enable them to avoid contractual arrangement they do not agree to or are uncomfortable with. However, given the extent to which modern consumers rely on internet-based products and services, it may be unreasonable to argue

[3] *Privacy Act 1988*, Australian Privacy Principle 3.3

[4] OAIC, Australian Privacy Principle guidelines, pp8-10.

that consumers who are unhappy with a business's contract terms services should simply 'walk away'. Ideally, consumers should be able to make choices in their dealings with service providers that allow them to enjoy the benefits of internet-based products and services without having to provide personal information for marketing purposes.

Improving the communication of privacy information depends upon a closer consideration of the function of privacy policies and notices. Under the Privacy Act, these communications have the basic function of setting minimum requirements on information to be available to individuals.[5] However, the function of privacy communications can be seen more broadly. In developing improvements in the way service providers communicate with consumers, policymakers and service providers should consider these additional functions of privacy communications:

- To provide consumers with information that facilitates privacy options
- To provide a means by which consumers can easily compare companies, facilitating competition on privacy practices

- To provide a public information resource for regulators, organisations, companies, researchers and other interested parties
- To provide commitments to consumers and accountability regarding privacy protections.

By improving their communications with consumers, service providers can strengthen the protection of consumers' privacy interests in the digital age.

Improving privacy communications

The approach recommended by this project is pragmatic. In an ideal world, consumers would always enter relationships with service providers with express, informed consent with respect to how their personal information is handled; however, this high standard of consent may not be realistic in every context and situation. Even where the presentation of information is perfectly pitched to inform consumers there is no guarantee that consumers will make the effort to inform themselves. The best that a service provider can do is to maximise the *opportunity* of the consumer to provide free and informed consent.

This research identifies a complex interplay of obstacles that come between the consumer and the provision of free and informed consent. A consumer must first locate or be made aware of privacy information. The consumer must then read that information. The likelihood that a consumer will read a privacy communication is influenced by the length and perceived complexity of the communication. The likelihood of reading is also influence by the extent to which consumers are incentivised to read communications – if consumers cannot exercise any options on privacy as a result of communications, other than to walk away from a contract, they have little reason to read them.

Having read privacy information, consumers must then understand what it means. Understanding is influenced by the complexity of the information and consumers' level of background knowledge. The

[5] *Privacy Act 1988 (Cth)*, Australian Privacy Principle 1.3 and 5.

perception of complexity is affected by the inherent complexity of underlying practices, and the means by which the information about those practices is communicated. Currently, the language used to describe practices is often vague, legalistic, overly technical and biased towards service providers in its depiction of information practices. Finally, where consumers understand details about a service provider's practices, they must then be able to form a coherent view on the relevance of that information to them in order to make good decisions.

Some commentators believe that the attempt to seek the informed consent of consumers is unrealistic, arguing that it is impossible to adequately explain to consumers the complexities of companies' information-collecting practices.[6]

Even where the details are explained, vital information may lie in nuances and details that are unlikely to be discerned by consumers with little knowledge of industry practices.[7] Further, the more complicated and detailed information is, the greater the effort consumers must go to in order to read and understand that information. The scale of the learning task – which can be conceptualised as a cost to the consumer – makes it unlikely that consumers will dedicate the necessary time and energy in attempting to come to terms with a service provider's privacy practices and their likely consequences.

Privacy commentators have also drawn attention to the difficulty consumers have in accurately assessing risk.[8] According to prospect theory, a central theory within behavioural economics, people tend to overvalue short term benefits when compared to long term risks. Since long term risks relate primarily to how access to personal information impacts upon privacy, and short term benefits relate to the enjoyment of products or services, individuals are likely to undervalue their privacy in entering transactions with service providers.

However, even where consumers are able to accurately assess the trade-off between risk and benefit, it seems likely that many people would be prepared to accept the terms set by service providers on the basis that the digital products and services they provide are perceived to be essential.[9] That is, while consumers may be informed about the consequences of entering a contract, they may feel that they have little choice but to accept a service provider's terms and conditions.

Despite arguments that true consent is either impossible to achieve or does not, by itself, result in improved privacy protection, this research proposes that the standard of consent is in fact open to significant improvement, and that this is an important factor, alongside the improvement of the communication of privacy information, in the development of a more effective framework for the protection of privacy.

---

[6] See for example H Nissenbaum, 'A Contextual Approach to Privacy Online' (2011), 140 *Daedalus, Journal of the American Academy of Arts & Sciences*, pp32-48; D Solove, 'Privacy Self-Management and the Consent Dilemma'(2013), 126 *Harv. Law Rev.* 1880; R Sloan and R Warner, 'Beyond Notice and Choice: Privacy, Norms and Consent' (2013), *Suffolk University Journal of High Technology Law*.

[7] As noted by H Nissenbaum, see note 6, p36.

[8] See in particular Sloan and Warner, and Solove, see note 6.

[9] R Joergensen, 'The unbearable lightness of user consent' (2014), 3(4) *Internet Policy Review*.

This report provides simple recommendations to improve the standard of communications and consent. One is by drawing consumers' attention to specific pieces of information that are likely to inform consumers' decisions to give or withhold consent. The authors contend that adequately informed consent does not require the consumer to understand the full complexity of information handling processes, but rather to have an awareness of how those processes are likely to have an impact on the consumer's interests.

Fieldwork research that focuses on how consumers behave in the digital environments in which they make decisions regarding privacy should be conducted to determine the relevance of particular information about privacy on how consumers make decisions. Fieldwork should also be used to test, refine and supply empirical data on the effectiveness of delivering privacy information and options in different formats and platforms in adequately engaging the attention and participation of consumers.

The standard of communication can also be raised by improving the actionability of privacy communications. Where consumers are provided with meaningful options, consumers are encouraged to be active participants in their relationships with service providers, rather than passive 'acceptors' of whatever terms and conditions service providers choose to impose. Improving actionability provides consumers with an incentive to read and understand privacy communications as well empowering consumers to take control over their personal information.

Improving the communication of privacy information narrows the gap in knowledge between service providers and consumers. Many consumers unquestioningly accept the terms of consumer contracts, which has significant implications for the protection of privacy and ability of the consumers to protect their own interests. Consumers 'give away' large amounts of their information to companies, that may then be aggregated, shared or sold to third parties. It may also be analysed to reveal consumers' purchasing habits and interests, often without full knowledge that companies are doing so. Closing the information gap would improve the opportunity for informed consent and drive a market environment in which consumers are able to discriminate between service providers on the basis of their privacy practices.

The means by which improvements in the communication of privacy information should be measured should not be determined solely by the extent to which it provides for informed consent. Improving the communication of privacy information should contribute to a raft of improvements in the relationship between service providers and consumers: it is likely to incrementally improve the knowledge-base of consumers about information-handling processes and contribute to a higher level of consumer trust in service providers; to help generate privacy norms with regard to personal information; to improve service providers' communications strategies and approaches to privacy; and help establish a basis upon which service providers compete and innovate with respect to privacy.

2. Summary of Recommendations, Options and Issues

2.1. The communication of privacy information

To better inform consumers, privacy communications should:

1. Be more accessible and visible for consumers
2. Include relevant, interesting and helpful privacy information that is brought to consumers' attention.
    - A fieldwork study should be developed to test which information is important to consumers
    - Descriptions of technical, administrative and functional uses of personal information should be clearly distinguished from commercial uses of personal information
3. Provide consumers with flexible, meaningful and actionable privacy choices at the time consumers read the information
    - Fieldwork should test consumers' engagement with different types of privacy options and controls
    - Using a behavioural economics approach, fieldwork should test how consumers engage with information: e.g. consumers' perceived cost of learning privacy information; the importance of framing effects and other cognitive biases in influencing consumer decisions
4. Be innovative in dealing with informational complexity. Innovations could include layering of privacy information, use of visual aids, diagrams, multi-media and/or an icon system
    - Fieldwork should test the efficacy of different privacy communication models

In improving communications with consumers, service providers should also take into account:

5. The extent to which consumers comprehend the information that is provided to them
    - Fieldwork should test how well consumers understand the language and information used in privacy communications
    - Fieldwork should test the background knowledge of consumers regarding the ways service providers collect, process and analyse personal information
6. Whether the information provided to consumers is neutral and balanced
7. Whether it is necessary for privacy communications to appear in the context of contractual terms and conditions. Where privacy communications are intended to form a contract with the consumer, this should be made clear
8. Different industry sectors should consider ways to standardise elements of privacy communications, enabling consumers to compare between service providers on the basis of their privacy practices.

2.2. Consent and consumer empowerment

Policy options for improving consent and informed decision-making

1. To improve the level of consumer control and the protection of privacy, the range of practices that require consumer consent should be expanded and awareness of those controls should be improved
    - Service providers should avoid bundling consent
2. With regard to consent, consumers should be informed, and have choices and controls with respect to information that they are likely to find important, in particular:
    - The sale of their information
    - The aggregation of their information
    - The analysis of their information
3. Default settings should favour the privacy of the consumer
    - Fieldwork research should provide data with respect to the differences between methods of obtaining consent (eg opt-in versus opt-out)
4. Service providers should maximise the opportunity for consumers to provide informed consent
5. The giving of consent should be separated from any browsewrap and clickwrap contracts
6. Consumers should be able to withdraw consent for the use of their personal information
7. Consumers should be provided with effective notice and privacy controls where service providers change their privacy policies.

2.3. Contract and consumer law

Key issues:

1. The legal validity of clickwrap and browsewrap contracts
2. Whether privacy interests should be subject to clickwrap and browsewrap contracts
3. Whether privacy policies should be contractual – are contracts required by service providers in order to collect and use personal information in the ways described in privacy policies?
4. The terms in consumer contracts and privacy policies that may be considered 'unfair'? For example:
    - Terms that attempt to obtain informed consent for overseas disclosure for the purposes of Australian Privacy Principle (APP) 8[10]
    - Terms providing for extensive collection and usage rights, including the disclosure of personal information to multiple, often unidentified, third parties
    - Terms that state that the service provider is not responsible for the privacy practices of third parties
5. Possible aspects of unconscionable conduct under Australian Consumer Law when considering privacy policies as a whole:
    - Clauses exploiting obvious inequality of bargaining power
    - Unilateral right to vary contract
    - Non-negotiability

[10] *Privacy Act 1988 (Cth)*, Australian Privacy Principle 8

Table of Contents

3. Project Outline

This report considers how to improve the communication of privacy information to consumers. It focusses on four types of service provider that are the subject of community concerns: web browsers, search engines, social media and app advertisers.[11]

While there is a level of community concern, there is also research that suggests that social media providers have privacy policies and supporting materials that are transparent and user friendly compared to other industry sectors.[12]

Comparative analysis of the presentation and content of privacy information is intended as a means to equip industry, regulators and consumer groups with knowledge of legal and ethical problems associated with the content and provision of privacy policies. It provides an evidence base upon which to identify specific obstacles to the provision of informed consent. A clear analysis of specific areas for improvement provides a practical means by which industry, regulators and consumer advocacy groups can develop improvements to the manner in which privacy information is communicated, to protect and empower consumers.

The report is intended to establish a platform for fieldwork to test consumer responses to different models by which privacy information is presented to consumers. Fieldwork would allow for the collection of rich data on how consumers make decisions on the basis of the presentation of privacy information. Fieldwork would include the testing and refining of templates for privacy communications and controls, and would lead to recommendations to service providers and policymakers regarding the adequate and effective presentation and communication of privacy information that consumers can act on.

The body of this report includes five main sections:

- **Background**
    - **Commercial and technological context**
    - **Industry context, codes and guidelines**
    - **The Australian privacy framework**
- **Issues relevant to the communication of privacy information to consumers** – an identification of issues relating to the ability of consumers to give informed consent for the collection and use of personal information
- **Privacy Policy analysis** –analysis of 16 privacy policies in the communications sector
- **Consent and consumer empowerment** – legal and policy issues connected to the provision of consent
- **Appendix**
    - **Privacy Policy comparative analysis** – comparison of privacy policies

[11] Deloitte report, Australian Privacy Index 2015, p11. The industries of telecommunications and social media were identified by consumers as the most identified with privacy issues.

[12] See above, p15.

- **Accessibility of Privacy Information**

This report also includes sections on:

- **Contract and consumer law**
- **Basic concepts in contract law**
- **Legislation dealing with unconscionable conduct**

Research Methodology

Stage 1: Legal and policy research

- A literature review was conducted on information privacy, privacy policies and consumer consent
- Legal research was conducted into contract theory, consumer law and information privacy law
- Contract law research was conducted to provide information regarding valid contract formation
- Consumer law research was conducted to provide background information on fairness and unconscionability in consumer contracts
- Information privacy law research was conducted to provide information on service provider requirements in privacy statements

Stage 2: Privacy policy analysis

- Sixteen privacy policies were examined across four different communications industry sectors
- Individual privacy policies within industries were selected to table a range of information collecting practices, focusing on companies with relatively large customer bases

Privacy policies were examined on the basis of:

- Accessibility and visibility
- Length
- Contractual issues
- Complexity and use of language
- Standard of privacy protection

Stage 3: Consultation

- Industry and Regulator Reference Group met to discuss issues relating to the communication of privacy information to consumers (2 September 2015)
- Industry and Regulator Reference Group was consulted on draft report
- Industry and Regulator Reference Group was represented by the Association of Data-driven Marketing and Advertising (ADMA), the Interactive Advertising Bureau (IAB) Australia, Google, the Office of Australian Information Commission (OAIC) and the Australian Competition and Consumer Commission (ACCC).

4. Background

4.1. Commercial and Technological Context

The information age has seen a dramatic and rapid change in communications technologies and information exchange. The widespread adoption of the internet and the global expansion of communications networks have connected individuals, businesses and governments in a way not before seen.[13] Vast amounts of information, including information about people, is now capable of being collected, stored, aggregated, analysed, shared and traded. There are benefits to businesses, governments and individuals stemming from the availability of personal information, but also new challenges for the protection of privacy.

The benefits of the information age include the free flow of information between individuals and entities, and the free flow of information across national borders. The flow of information has benefitted government administration and the provision of services, and has helped to enable the development of global e-commerce and improved user convenience. It has also provided a basis for behavioural advertising and other business models – means by which search engines, social media and other internet-based providers have been able to monetise their services. Behavioural advertising has enabled greater efficiency in the delivery and response to advertising.

The availability of information about consumers, the development of technologies through which this information is collected, and business models that require the collection and use of this information, represent significant challenges for the protection of privacy and the establishment of an effective privacy framework that is flexible and attuned to technological change.

In the information age, information about consumers is persistent, abundant and easily accessed.[14] Consumer information is collected regarding shopping habits, web-browsing habits, search inquiries and geolocation. These data have the potential to reveal a substantial amount about the lives of internet users, including 'information about health, education, credit history, [and] sexual or political orientation.'[15] Data sets are also being linked, aggregated and analysed to create new information about individuals that provide advertisers with a more accurate picture of the individual's interests and habits.

The significance of this data for consumers, from a privacy perspective, depends on the extent to which this information is genuinely anonymous. An argument may be made that information about a consumer that is not readily identifiable is of no interest to the consumer and, therefore, does not require the consumer's consent. On the other hand, some consumers may feel differently – that the

[13] In 2012-13, a survey conducted by the Australian Bureau of Statistics indicated that 83% of Australians over 15 had accessed the internet within the last 12 months.
(http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/8146.0Chapter32012-13)

[14] See for example, Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice (ALRC Report 108), vol.1, p 392.

[15] See above.

level of risk that resides in purportedly anonymous information warrants a level of consumer control. The fact that the information about consumers is commercialised and used for marketing purposes may also give rise to the argument that consumers have a legitimate interest in their information and that they should be consulted with respect to its commercial exploitation.

Changes in business models and organisational practices have taken advantage of and driven technological change. For some businesses the use of personal data – whether for sale to third parties, advertising, or for tailoring their own services – is the core asset in their business model.[16]

Social media sites such as Facebook have enabled individuals to readily share personal information, establishing the basis for a business model in which personal information enables the targeting of third-party advertising and the monetisation of social media service. Online advertising networks use cookies and other tracking technologies to collect browsing histories of individual consumers and deliver targeted advertising to them that reflects their interests. In 2010, US$25 billion was spent on online advertising in the United States, representing 18 per cent of all advertising spending.'[17]

The collection and analytical processing of personal information is powerfully incentivised. In 2008, Google purchased advertising network DoubleClick for $3.1 billion. In 2011, it saw advertising revenues of $36.5billion, with $10.4billion coming from non-Google sites in its ad network.[18]

The internet advertising market is expected to grow at an average rate of 9.4 per cent to reach $4.9 billion by 2017. Advertising on mobile devices is predicted to experience a 25.7 per cent compound annual growth rate to reach $244 million or 5 per cent of the total online advertising market.[19]

Changing business models and changes in the use of technology have created a number of perceived risks related to unanticipated uses of personal information, monitoring and trust.[20] A number of high profile security breaches have undermined the trust of individuals in organisations.[21] The use of personal information by cyber-criminals has also created a general loss of trust in online engagement and e-commerce.

With changed business models and uses of technology, and the increasingly complicated means by which value is extracted from consumer information, it seems less and less possible for consumers to gauge the consequences of the potential uses of information at the time it is collected. Service providers attempting to maximise the value of the information they collect face a challenge of

---

[16] See note 14, p 152. One such company is Acxiom, which promotes itself as:
'A global leader in helping companies maximize the value of information. Our innovative information management solutions provide critical insights into consumers that help companies acquire and build stronger, more profitable relationships with their customers.'

[17] McKinsey & Company, The Impact of Internet technologies: Search, p23.

[18] *The Guardian,* 23 April 2012: 'Double click tracking trackers cookies web monitoring.' http://bit.ly/1RH9afj

[19] Pwc, Outlook, Australian Entertainment and Media 2013-2017, p92.

[20] See for example OECD report, The OECD Privacy Framework (2013), p66-69.

[21] See for example note 14, p395.

accurately communicating to consumers, who often lack adequate background knowledge, how their data will be used, while attempting to maintain the trust of the consumer.

4.2. Industry context, codes and guidelines

This report focuses on four industries within the digital and communications sector that have attracted public attention for their privacy practices: search engines, social media, mobile app advertisers and web browsers. Background information on these sectors, prominent business models, and information handling practices is provided in 6. Privacy Policy Analysis.

Privacy concerns include the commercial purpose to which personal information is being put,[22] the transparency of the information that is being provided to consumers with respect to those uses,[23] and the difficulty faced by the consumer in providing informed consent for the use of personal information.[24]

The service providers in this study do not necessarily operate as simple and distinct industries with clear one-on-one relationships with consumers. They instead often operate with related entities that may include 'third parties'– entities that the consumer does not have a direct contractual relationship with. Mobile app publishers, for example, work within complex 'ecosystems' in which the personal information of consumers may be collected by publishers, third party advertisers or advertising networks – companies that connect advertisers and publishers.[25]

This research focuses on consumer services that have a direct relationship with consumers and that have the most obvious responsibility for providing contract and privacy information to consumers. Despite this focus, there may be other entities within these business and information ecosystems that share a responsibility for making information about privacy available to consumers. All the entities within these business ecosystems are likely to have responsibilities to make information available about their personal information practices.

The Australian Privacy Principles (APPs) outline the specific obligations of entities with respect to the collecting and handling of personal information. In addition to compliance with the APPs, specific industries may also choose to develop and apply their own self-regulatory codes. An industry can choose to develop and register an APP code with the Information Commissioner, according to specifications in the Privacy Act.[26]

4.2.1. Association of Data-driven Marketing and Advertising

[22] See for example J Rule, *Privacy in Peril*, p95-97.
[23] See for example Nissenbaum, see note 6.
[24] See for example Solove, see note 6.
[25] A description of mobile app ecosystems can be found in Federal Trade Commission report (US), 'Mobile Apps for Kids': Current Privacy Disclosures are Disappointing' (2012), p3.
[26] *Privacy Act (Cth)1988*, sect 26.

The principal industry body for information based marketing in Australia is the Association of Data-Driven Marketing and Advertising (ADMA). According to its website, the ADMA has over 600 member organisations including major financial institutions, telecommunications companies, energy providers, leading media companies, travel service companies, airlines, major charities, statutory corporations, educational institutions and specialist suppliers to the industry including advertising agencies, software and internet companies.[27] The ADMA administers a self-regulatory industry code, the ADMA Code of Practice, introduced in September 2015.[28]

4.2.2. Australian Digital Advertising Alliance

Online behavioural advertising is subject to a separate self-regulatory scheme administered by the Australian Digital Advertising Alliance (ADAA), a group of business and industry associations in the online advertising sector. The ADAA publishes the Australian Best Practice Guideline for Online Behavioural Advertising (the 2011 Guidelines).[29] The scheme is based upon a similar scheme that operates in the United States. The US body, the Digital Advertising Alliance (DAA), formed in response to a report by the Federal Trade Commission which recommended that consumers should be able to easily opt out from receiving online behavioural advertising (OBA). The DAA created a 'clickable' OBA icon called AdChoices for companies to place alongside behavioural ads.

The founding members of ADAA are the Australian Association of National Advertisers (AANA), ADMA, the Australian Interactive Media Industry Association, the Communications Council, the Australian Interactive Advertising Bureau, the Media Federation of Australia (MFA), the Internet Industry Association, Google, Microsoft, NineMSN, Telstra Advertising Network, Network Ten Digital and Yahoo7.

Signatories also include Radium One, Amobee, Fairfax Digital, News Corp Australia, Mi9, REA, Eyeota, Adobe, Xaxis, Carsales Network and Yahoo7.[30]

The 2011 Guidelines outline obligations with respect to OBA data, which is defined as 'data on web browsing activity of an internet-enabled device which allows the device to be added to one or more pre-defined interest categories.' The Guidelines specify that if a third party combines OBA data with personal information, then OBA data must be treated as personal information in accordance with the Privacy Act. The Guidelines create obligations on providers of 'third party OBA', which is advertising provided to users on the basis of their web browsing history across websites that are not associated with or are not owned by the advertiser. The obligations on advertisers include:

- Providing clear and comprehensible notice on their websites describing their practices in relation to the collection and use of data for Third Party OBA purposes,

[27] The New ADMA - http://bit.ly/1UsdfaO
[28] ADMA Code of Practice - http://bit.ly/1SlBIZn
[29] ADAA Best Practice Guideline - http://bit.ly/1ol5g0Z
[30] About ADAA - http://bit.ly/1PEF7AC

- Providing web users with an easy to use mechanism to withdraw consent with respect to the collection and use of data for Third Party OBA purposes,
- Providing web users with easily accessible mechanisms for consumers to lodge complaints directly to entities
- Listing themselves on an industry-developed website linked to the OBA disclosure.

The ADAA runs a 'Your Ad Choices' scheme which provides a mechanism by which consumers can opt out of OBA using a one-click process. As of 30 July 2015, thirteen companies are participating in this program.[31]

4.3. Privacy and information privacy law

4.3.1. Definition of 'personal information'

Australian consumers receive protection of their personal information in accordance with the Privacy Act 1988. The Act protects the privacy of individuals by creating a number of obligations on private and government organisations regarding the handling of 'personal information,' which is defined as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable'.[32]

The Office of the Australia Information Commission (OAIC) has not provided detailed guidance on the types of information that may be considered 'reasonably identifiable'; however, it has stated that in some circumstances internet protocol addresses, unique device identifiers and other unique identifiers will be considered to be personal information.[33]

In a 2009 report, the US Federal Trade Commission (FTC) concluded that information that is often labelled as 'non-personally identifiable' by participants in the behavioural advertising sector ought to be treated as identifiable on the grounds that this information, while it may be anonymous in isolation, is capable of being linked to information that identifies an individual.[34] The FTC found that information labelled as non-personally identifiable (including IP addresses and cookie information) often carries a privacy risk that is similar to personally identifiable information.

A legal ruling by the UK Information Commissioner supports the principle that information such as IP address that uniquely locates an individual in the online world should be regarded as personal information.[35]

---

[31] Your Online Choices, Opt Out - http://bit.ly/1pJpaUr

[32] *Privacy Act 1988* (Cth), s6.

[33] OAIC report, Mobile privacy: A better practice guide for mobile app developers (2014), p3.

[34] Federal Trade Commission (US) report, Self-Regulatory Principles for Online Behavioral Advertising (2009), p20-25.

[35] United Kingdom Government Information Commissioner's Office, Data Protection Act 1998 Legal Guidance (2001):

This report adopts the position, based upon the positions of these regulators, that information about a person that is linked to that person's computer or other digital device, for example by IP address or unique device ID, is sufficiently identifiable and should be regarded as personal information.

4.3.2. The information privacy framework

Australian government agencies and private sector organisations with an annual turnover in excess of $3 million must comply with the Australian Privacy Principles ('APPs'). The thirteen APPs cover the collection, use, disclosure and storage of personal information; the requirement for privacy policies and notices (APP1.3 and APP5); the purposes for which personal information may be shared (APP6); the ability of individuals to access their personal information (APP12) and have inaccurate information corrected (APP13); cross-border disclosure of personal information (APP 8); and the use and disclosure of personal information for the purpose of direct marketing (APP 7).

The Australian Privacy Act, and personal information legislation in many international jurisdictions, is based on principles proclaimed by the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ('OECD Privacy Guidelines').[36] Despite some differences across jurisdictions, the OECD Privacy Guidelines and other international instruments such as the APEC Privacy Framework, have helped to ensure a level of uniformity across the globe. However, US entities are not subject to federal legislation for the protection of personal information. Most major US companies that handle personal information participate in self-regulatory schemes that establish guidelines for the protection of privacy. The Federal Trade Commission (FTC) plays an important role in the protection of consumers' privacy by making US companies accountable for misleading statements in their privacy policies. The FTC has also played an important part in privacy reform measures in the US by developing principles and policies that have been adopted by different industry sectors, such as the online behavioural advertising sector.[37]

Under Australian law, companies that collect the personal information of consumers have a number of other legal obligations to consumers. Australian Consumer Law and contract law are relevant to consumers' privacy rights because the legal mechanism by which companies formally facilitate the collection and use of consumers' personal information is contractual. The protection of consumers' privacy and personal information depends in part on whether the formation and substance of consumers' agreements with service providers can be considered legally valid. Improving the privacy protection of consumers is likely to require a shift in approach to the way in which consumers give consent for the collection and use of personal information.

'information [such as IP address] is, nevertheless, personal data. In the context of the on-line world the information that identifies an individual is that which uniquely locates him in that world, by distinguishing him from others.'

[36] See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - http://bit.ly/1gaZQzY

[37] FTC report, 'Protecting Consumer Privacy in an Era of Rapid Change' (2012).

While Australians do not have an express legal right to privacy, the right to privacy is often considered to be a fundamental right of citizens living in a democracy. In Australia, privacy is to some extent protected by other laws: for example, law on breach of confidence and defamation has been applied in a number of circumstances that protect privacy.[38]

At the time of writing, the Australian Law Reform Commission (ALRC) was giving consideration to a statutory tort for 'serious invasions of privacy'.[39]

4.3.3. The function of privacy communications under the Privacy Act

Under the Privacy Act, entities have two separate obligations regarding the disclosure of information about privacy practices. APP 1.3 requires entities that collect personal information to have a 'clearly expressed and up-to-date policy about the management of personal information'. Entities are also required to take steps to ensure that individuals are notified when personal information is collected and to provide details about the collection (APP 5.1). If an individual has already been made aware of relevant information, the individual does not need to be notified again.

APP 1.4 prescribes the information that must be included in privacy policies. It includes: types of personal information; storage of personal information; purposes for which personal information is collected and used; how individuals can access personal information; how the individual can complain; and details regarding overseas disclosures of personal information.

Notifications to individuals about the collection of personal information must be provided under APP 5.1. The information that must be provided is the same information that is required for privacy policies, but also includes: information that draws the individuals attention to details in the entity's privacy policy; whether personal information is collected from someone other than the individual; whether the collection is authorised under an Australia law or court order; the consequences, if any, of the individual not supplying personal information; and with whom the entity is likely to share the personal information.

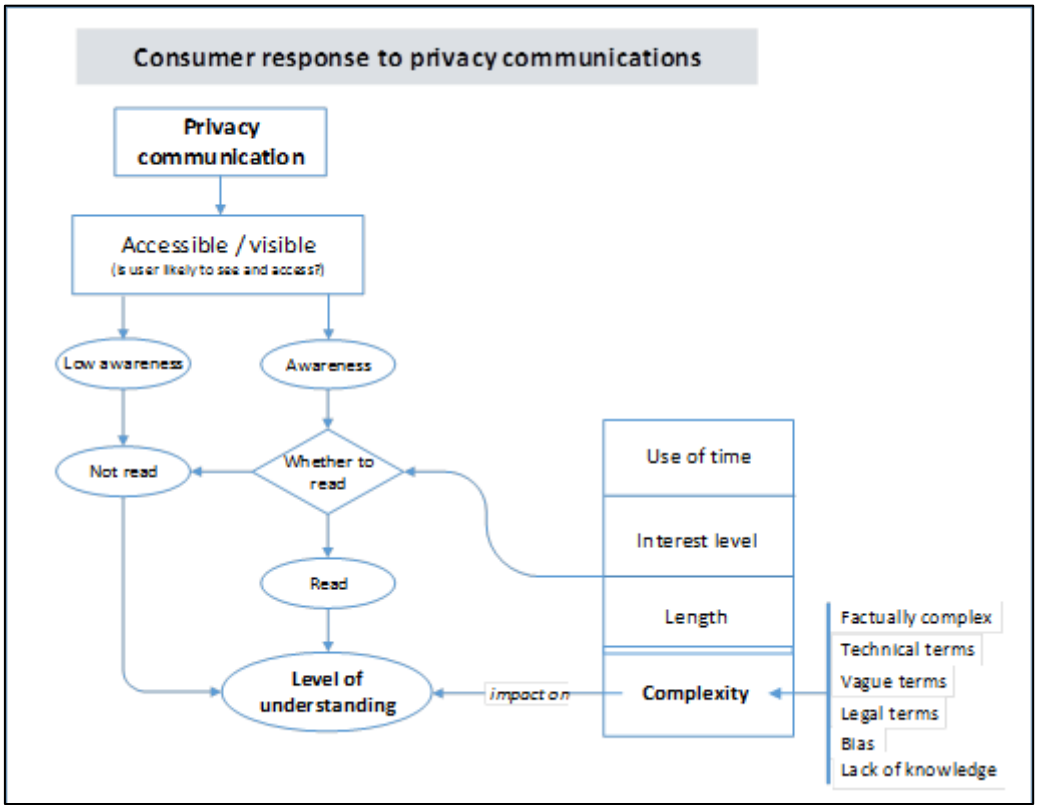
[38] For a relevant breach of confidence case, see *Giller v Procopets* [2008] VSCA 236 (10 December 2008); for a relevant defamation case, see *Ettingshausen v Australian Consolidated Press Ltd* [1995] NSWSC 176.
[39] See report, ALRC, Serious Invasions of Privacy in the Digital Era (2013) at http://bit.ly/21SBSMR.

5. Issues Relevant to the Communication of Privacy Information

Our analysis indicates a number of factors that have to be addressed to improve the protection of privacy and the ability of individuals to make informed decisions as consumers:

- Privacy policies are seldom read
- Accessibility and visibility of privacy communications
- Length of privacy communications
- Complexity of privacy communications
    - Complexity of information handling practices
    - Impact of complexity on decision-making
    - Clarity of language, use of legal language and industry terminology
- Lack of balance in description of practices
- Relevance of privacy communications to people
- Lack of necessary background knowledge and experience among consumers
- The cost to consumers of reading privacy policies.

In order for consumers to obtain the necessary level of knowledge, a sequence of factors must be satisfied: consumers must see privacy communications; they must read privacy communications; they must understand the words and concepts described in communications; and they must evaluate the information and compare the practices of service providers.



5.1. Privacy communications are seldom read

According to the Office of the Australian Information Commissioner (OAIC) Community Attitudes to Privacy survey (2013) (OAIC Survey Report), 44 per cent of Australians claim to read website privacy policies.[40] Another Australia-wide survey conducted in 2012 by the University of Queensland Centre for Critical and Cultural Studies found that 18 per cent of Australian internet users read privacy statements most or all of the time, with a further 18 per cent claiming to sometimes read them.[41]

5.2. Accessibility and visibility of privacy communications

On websites, privacy policies and contractual terms of service are usually included as hyperlinks (for example Appendix B, images 1 and 2).

On mobile devices, to access the privacy policies and licence agreements of mobile apps, users must first seek out more information about an app by clicking on a link within a website that displays the app (for example Appendix B, images 3-6).

The extent to which consumers read privacy policies is likely to be connected to how accessible privacy communications are and the extent to which they are brought to the attention of consumers. A consumer is more likely to read a privacy policy where it is prominently displayed or information about its existence is brought to the consumer's attention.

The type of platform – computer or mobile device – may influence the visibility of privacy policies and the tendency of consumers to access them. The display of privacy information on the small screens of mobile devices also presents a communications challenge (see Appendix B, images 3-6).

In the OAIC Survey Report, five per cent of respondents indicated that the reason why they do not read privacy policies is because they are 'hard to find'. While this may not seem significant in determining whether consumers read privacy policies, it may nevertheless be the case that privacy policies are not easy for many consumers to find. The typical display of a hyperlink labelled 'privacy' on most service providers' websites is not particularly prominent (see Appendix B, image 1).

It is reasonable to assume that when privacy policies are not actively brought to the attention of consumers, many would not know that they exist. In these circumstances, consumers do not consciously choose to avoid reading privacy policies – they are unaware of the privacy policy in the first place.

The question of accessibility and visibility has implications in contract and Australian Consumer Law (see 8.8.3 Incorporation of terms and 8.8.4 Vitiating factors).

[40] See note 2, p39

[41] Social Research Centre: University of Queensland report, Internet Privacy Research (2012), p26

5.3. Length of privacy policies

In the OAIC Survey Report, the main reason indicated by Australians for not reading privacy policies is that they are too long, with 52 per cent of respondents providing this as the reason for not reading them.[42]

A US study on privacy policies conducted in 2008 looked at privacy policies from 75 popular websites and concluded that the average time it would take a person, reading at 250 words per minute, to read a privacy policy is 10 minutes.[43]

The privacy policies in our study varied in length between 995 words and 7396 words, with an average of 3232 words. Based on an average reading speed of 250 words per minute, this would take the average reader about 4 minutes to read the shortest privacy policy, 29 minutes to read the longest, and 13 minutes to read a privacy policy of average length. For more information see 6. Privacy Policy Analysis.

5.4. Complexity of privacy communications

In the OAIC Survey Report, the second highest reason provided by Australians for not reading privacy policies is that they are too complex, with 20 per cent of respondents providing this as the reason they do not read them.[44]

In the opinion of the authors, privacy policies are indeed very complex, which is illustrated by the number of types of information that service providers collect and the uses to which that information is put (see 6.2.5 What information is collected?)

The difficulty for consumers in understanding typical privacy policies was tested by a 2008 US study which found that readers were only able to answer one-third of privacy-related comprehension questions correctly after reading a privacy policy.[45]

It seems likely that the perception of complexity is linked to the length of a privacy policy and the use of legal and technical language. These communications are also likely to be complex due to the inherent complexity of the practices they describe.

Complexity relates not only to whether consumers feel inclined to *read* privacy communications, but also to whether they are likely to *understand* them.

---

[42] See note 2, p41.

[43] A McDonald and L Cranor, 'The Cost of Reading Privacy Policies' (2008), *A Journal of Law and Policy for the Information Society*, p2.

[44] See note 2, p41.

[45] M Vail, J Earp and A Anton, 'An Empirical Study of Consumer Perceptions and Comprehension of Web Site Privacy Policies'(2008), 55 *IEEE Transactions on Engineering Management*.

5.4.1. Complexity of information handling practices

Our review of practices described in privacy policies provides an insight into the complexity of information collecting and processing practices, and the challenge of communicating this information to consumers (see also 6.2.5 What information is collected?)

A number of commentators contend that the complexity of some companies' information processing practices is too great for most consumers to understand, regardless of the quality of the presentation of the information.[46]

Helen Nissenbaum contends that the problem of complexity is particularly evident in the case of online behavioural advertising:

> The technical and institutional story is so complicated that probably only a handful of deep experts would be able to piece together a full account… Even if, for a given moment, a snapshot of the information flows could be grasped, the realm is in constant flux, with new firms entering the picture, new analytics, and new back-end contracts forged… Further, the complexity makes it not only difficult to convey what practices are followed and what constraints respected, but practically impossible.[47]

It seems likely that the problem is not one only of complexity, but of uncertainty. Even those who are collecting personal information for behavioural advertising do not necessarily know how personal information collected one day will be processed and exploited the next. This creates an obligation on the part of some service providers to regularly update their privacy communications. It also creates great difficulty in ensuring the continuation of consent of consumers who, while they may have accepted the initial terms and conditions of a privacy policy, may be unhappy with subsequent changes.

In order to deal with the complexity, attempts have been made to develop ways to summarise practices in the manner of nutrition labels.[48] Nissenbaum criticises the abbreviated approach to providing privacy information on the basis that an attempt to improve simplicity would also carry a significant loss of meaning.[49]

This report proposes that while it may not be possible to fully inform consumers about the details of service providers' practices it is nevertheless worth the attempt, and that a successful attempt

---

[46] See for example Nissenbaum and Solove see note 6; also J Turow, L Feldman and K Meltzer, 'Open to Exploitation: American Shoppers online and offline', report by Annenberg Public Policy Center of University of Pennsylvania; L Cranor and J Reidenberg 'Can User Agents Accurately Represent Privacy Notices?'(2002), at SSRN: http://ssrn.com/abstract=328860.

[47] Nissenbaum, note 6, at p36.

[48] For example, Privacy Bird: http://www.privacybird.org/

[49] Nissenbaum, note 6, at p36.

requires attention to that information which consumers are likely to find most relevant to them and their choices as consumers. See 5.6 Relevance of privacy information for consumers.

5.4.2. Impact of complexity on decision-making

According to an Australian Communications and Media Authority (ACMA) commissioned report on customer issues in communications markets, even where customers do have enough information and they understand that information, the complexity of the information may still result in confusion and poor decisions caused by 'information overload':

> Even in competitive markets, suppliers will possess market power if consumers are not well informed about products, supply alternatives, and feel unable/unwilling to switch between these alternatives or are unable to vary the privacy terms of the contract with the supplier. But behavioural economics adds another consideration to the information asymmetry problem. Even if consumers do have enough information, they might still make 'sub-optimal' decisions because of behavioural tendencies. To begin with there is the risk of 'information overload' that could result in confused consumers and worse decision-making. This was already recognised in conventional economic analysis but a 'behavioural' perspective places more emphasis on this limitation. [50]

5.4.3. Use of legal language and industry terminology

Where consumers attempt to read privacy communications, it is possible that the use of legal language and concepts may make them more difficult for many consumers to understand. Where consumers attempt to read privacy communications, it is possible that sometimes the use of legal language and concepts may make them more difficult for some consumers to understand (see 6.3.1 Meeting communications challenges).

However, most service providers reviewed present their privacy policies as contracts (see 6.2.2 Contractual issues). The language of most contracts is not crafted for easy comprehension. As contracts, privacy policies are intended to be legally robust instruments that protect against legal actions, not communications designed to be readable and informative. The contracts reviewed in this study tended to be overly comprehensive regarding descriptive elements that are unlikely to be of interest to the consumer, and too obscure on those points that are likely to be of interest to the consumer (see also 6.2.5 What Information is collected? and 6.3.1 Meeting communications challenges).

With respect to terminology, it is unavoidable that particular industries will develop their own technical terms. The use of terminology by service providers has the potential to cause confusion to consumers, particular if there is inconsistency in the use of terms. Where there is a high level of consistency, or standardisation in the use of terms, the use of industry terminology may in fact

[50] P Xavier, Behavioural Economics and Customer Complaints in Communications Markets (2011), p5.

improve consumers' level of understanding and assist consumers in comparing the privacy communications of service providers.

This study found a reasonably high level of consistency in the use of technical terminology (see 6.3.1 Meeting communications challenges).

5.5. Lack of balance in description of practices

Service providers draft their own privacy communications and it is, perhaps, unsurprising that in their communications with consumers that they should characterise their privacy practices in a positive light. However, the positive characterisation of privacy practices may be confusing for some consumers, who would benefit from information presented in a neutral way.

The information presented to consumers regarding the collection and use of personal information should not attempt to unduly persuade consumers about the benefits of providing service providers with their personal information. In order to be balanced, privacy communications should be more explicit in describing how service providers collect and process personal information in order to derive revenue through behavioural advertising.

Consumers should be presented with clearly expressed factual information that permits them to draw their own conclusions based upon those facts. It seems likely that persuasive language will be more influential on consumers who have a poor understanding of underlying practices and therefore little ability to 'read between the lines' (see also 6.3.1 Meeting communications challenges).

5.6. Relevance of privacy information for consumers

According to the OAIC Survey Report, 9 per cent of Australians indicate that they do not read privacy policies because they are too boring or they 'can't be bothered'.[51] Despite this low figure, it seems likely that most people would not find privacy policies particularly interesting.

The authors contend that the lack of interest that consumers have in reading privacy policies is likely to be strongly associated with the length and complexity of privacy policies, and that the validity of this claim should be tested through fieldwork.

The fact that many people do not read privacy policies, however, should not be seen as an indication that people are not interested in privacy. According to the OAIC Survey Report, Australians indicated a level of concern about the following practices and privacy issues:

- Many people do not like their personal information being sent offshore with 79 per cent believing this is misuse of personal information.
- Seventy-eight per cent of people are uncomfortable with their activities being 'covertly' monitored online.

[51] See note 2, p41.

- Many people (77 per cent) indicated a dislike of having information stored about them in order so that they receive targeted offers.
- The majority of people believe that websites (59 per cent) and smartphone apps (48 per cent) collect information about them and are uncomfortable with this practice.
- Many people have concerns about the security of websites with 78 per cent checking the security of websites before entering data.
- A large majority of people (60 per cent) have decided not to deal with an organisation because of privacy concerns.[52]

Many of these findings are echoed by independent research conducted by the ADMA in 2014. It found that:

- Only 36 per cent of consumers trust the companies they share information with.[53]
- Only 36 per cent of consumers are open to sharing personal information for rewards or offers.[54]

Research conducted by Price Waterhouse Coopers in 2012 paints a different picture, indicating that 73 per cent of consumers are willing to share personal information depending on the benefits they get in return.[55]

Given the high level of concern that Australians have regarding their privacy, it makes sense that people would be more likely to read privacy communications where information that is relevant to them, and reflects their concerns, is given prominence. Providing information that is relevant to consumers not only makes the information more likely to be read, but also arms consumers with the categories of information they require in order to make adequately informed decisions.

ACMA research on informed consent supports the contention that many consumers believe service providers have a deliberate strategy of keeping consumers in the dark with regard to important information.[56] Giving prominence to important and relevant information is therefore likely to improve the level of trust and confidence that a consumer has in a service provider.

The question of the relevance of privacy information is addressed to some extent by the requirements of APP 1.4 which specifies that privacy policies must include information on: types of personal information collected; how personal information is collected; the purpose for which

[52] See note 2, pp3-6.
[53] See ADMA report, Attitudes to Information Sharing, Privacy and Trust, p5.
[54] See above, p8.
[55] PWC Research about consumer privacy and information sharing: http://bit.ly/1LYUbyj
[56] ACMA report, Community research on informed consent (2011), p3:
'Consumers recognised that it was not always easy for them to give informed consent. In some instances, they believed that companies purposely make it difficult for consumers to comprehend the terms and conditions.'

personal information is used; how people can access and seek correction of personal information; and how people can complain.

We identify six additional categories of information that impact upon privacy and that consumers are likely to want to be informed about:

- Whether personal information is collected by third parties for advertising[57]
- Whether personal information is traded for commercial use[58]
- Whether personal information is used to target the consumer with behavioural advertising
- Whether the individual is able to exercise privacy preferences[59]
- Whether personal information is aggregated, analysed and used to form a profile of the individual
- Whether personal information is made available to advertising networks.

Future fieldwork research should identify the extent to which these categories of information are important and interesting to consumers, whether consumers find value in other information, and how to effectively communicate this information to consumers.

5.7. Lack of necessary background knowledge and experience among consumers

The ability of a consumer to understand privacy communications is likely to depend upon their level of background knowledge with respect to information privacy law, and how different communications industries collect and use personal information.

A 2005 US study found that Americans had a low level of understanding of basic practices relating to privacy.[60] For example:

- 64% didn't know that a supermarket is allowed to sell information about what consumers buy to other companies.
- 75% do not know the correct response – false – to the statement, 'When a website has a privacy policy, it means the site will not share my information with other websites and companies.'

[57] See also ADMA report, see note 53, p4. This report highlights the fact that while consumers 'share' their information with third parties, they are somewhat uncomfortable about this practice.
[58] See note 53. The report cautions 'against selling personal information for financial benefit', p4.
[59] See note 53. The report recommends that service providers 'Help consumers feel in control by giving them options,' p4.
[60] J Turow, L Feldman and K Meltzer, 'Open to Exploitation: American Shoppers online and offline', report by Annenberg Public Policy Center of University of Pennsylvania, p3.

The same study found that many Americans are misled by the label 'privacy policy', with many thinking that privacy policies are commitments to consumers about privacy, as opposed to being legal documents stating how the company will use personal information. The study recommended to the Federal Trade Commission that the term 'privacy policy' be replaced with 'using your information'.[61]

Without an adequate level of background knowledge a consumer is likely to find it difficult to make sense of information relating to privacy, and to distinguish between practices that are relatively 'responsible' or 'irresponsible'. Consumers are likely to require basic understanding of such things as behavioural advertising, advertising networks, cookies and IT security, in order to understand the merits of a particular service provider's privacy policy.

The ability of consumers to understand privacy information is likely to improve if they are provided with consistent information using standard defined terminology. Consistent formatting and presentation of privacy policies should also assist consumers to compare between privacy policies, and make better informed decisions.

The particular background of the consumer – which can be categorised in terms of age, education, language spoken and level of online experience – is also likely to be a factor in how consumers understand privacy information. The privacy communications of service providers should be flexible and adaptable enough to inform a broad range of consumers.

5.8. The time cost to consumers of learning privacy information

In order for consumers to properly inform themselves before entering into commercial relationships with providers, they must take advantage of whatever information is provided to them. Learning the information that is necessary to arrive at an informed decision incurs a cost that is borne by the consumer.[62] The longer and more complicated privacy information is the greater the cost to the consumer of attempting to learn that information. Other factors may also add to the cost such as the use of legal terms, vague and uncertain terms, and how text is presented. While consumers bear a cost in terms of frustration and confusion in attempting to understand privacy information, a measurable means of calculating the cost to the consumer is by estimating the length of time it is likely to take the average consumer to read and understand privacy information. This length of time can be characterised as an 'opportunity cost' – the value of opportunity the consumer must sacrifice in order to perform the task of reading and understanding.

It is reasonable to assume that as the cost of reading a privacy policy increases, the less likely it is that a consumer will read a privacy policy. The current cost of reading privacy policies is likely to be

[61] See above, p30.

[62] See note 43. The researchers considered the question of the 'opportunity cost' represented by consumers reading privacy policies.

too high for most consumers – in other words, consumers get greater value from doing something else. However, the failure to read a privacy policy incurs a different cost because the lack of information that the consumer learns affects the consumer's ability to make optimal decisions to protect privacy.

Fieldwork research into privacy communications should consider how to present information to consumers that has a low opportunity cost for the consumer and that is high in informational value, thus increasing the likelihood that consumers will engage with them.

To better inform consumers, privacy communications should:

1. Be more accessible and visible for consumers
2. Include relevant, interesting and helpful privacy information that is brought to consumers' attention.
    - A fieldwork study should be developed to test which information is important to consumers
    - Descriptions of technical, administrative and functional uses of personal information should be clearly distinguished from commercial uses of personal information
3. Provide consumers with flexible, meaningful and actionable privacy choices at the time consumers read the information
    - Fieldwork should test consumers' engagement with different privacy options and controls
    - Using a behavioural economics approach, fieldwork should test how consumers engage with information: eg. consumers' perceived cost of learning privacy information; the importance of framing effects and other cognitive biases in influencing consumer decisions
4. Be innovative in dealing with informational complexity. Innovations could include layering of privacy information; use of visual aids, diagrams, multi-media and/or an icon system.
    - Fieldwork should test the efficacy of different privacy communication models

In improving communications with consumers, service providers should also take into account

5. The extent to which consumers comprehend the information that is provided to them
    - Fieldwork should test how well consumers understand the language and information that is provided to them
    - Fieldwork should test the background knowledge of consumers regarding the ways service providers collect, process and analyse personal information
6. Whether the information provided to consumers is neutral and balanced
7. Whether it is necessary for privacy communications to appear in the context of contractual terms and conditions. Where privacy communications do intend to form a contract with the consumer, this should be made clear
8. Different industry sectors should consider ways to standardise elements of privacy communications, enabling consumers to compare between service providers on the basis of their privacy practices.

6. Privacy Policy Analysis

The material in this section is based upon an analysis of sixteen privacy policies. A summary of the analysis can be found in Appendix A – Privacy policy comparative analysis table. The analysis in this table is not intended to be a comprehensive analysis of all parts of these privacy policies, but rather a consideration of a selection of key issues.

This section supplements and informs recommendations and findings in 5. Issues Relevant to the Communication of Privacy Information.

6.1. Four communications sectors

This project has a focus on the privacy communications of four communications industry sectors: mobile app publishers, web browsers, search engines and social media sites. Different sectors tend to support different types of business models, and different business models utilise personal information in different ways. However, within these environments, some service providers depart from typical business models by promising greater privacy for consumers as an aspect of the service offering.

6.1.1. Mobile app publishers and developers

The primary role or function of app publishers and developers is to design, develop and bring apps for smart phones and devices to market. These apps are made available through sites such as the Apple App Store (for Apple devices) or Google Play (for Android devices). An important means by which many app publishing companies monetise their products is by making their apps available to advertising networks who deliver the marketing communications of third party advertisers within apps. App publishers receive payment from advertisers via advertising networks. The amount of revenue app publishers receive depends upon the success of advertising within their apps, which is usually measured by the number of 'clicks' they receive.

The privacy concerns that relate to app publishers can be generalised to the larger industry ecosystem. The manner in which personal information is distributed and processed within those ecosystems depends upon the agreements those industry participants have with each other.

From the perspective of the consumer who is considering purchasing an app, the most prominent party within the app ecosystem is likely to be the app publisher. It is the app publisher's privacy policy that is available to the consumer when downloading an app. However, the terms associated with an app may permit third parties to collect personal information in connection with the delivery of behavioural advertising to the consumer.

Where a consumer has a concern about third party behavioural advertising within this context, the consumer is likely to have to refer to the privacy policies of third parties, rather than the privacy policy of the app publisher itself. App publishers tend to refer to the existence of third parties, but rarely take responsibility for their practices or policies.

In order for the consumer to get a full picture of how personal information is collected and used, the consumer would also need access to the privacy policy of the advertising network or networks that act as intermediaries between advertisers and app publishers.[63]

[63] See also FTC report, note 25.

6.1.2. Web browsers

Web browsers are software applications that are required for computer users to access information resources on the World Wide Web. The global market in browsers is dominated by a small number of players. Technology companies that offer web browsers do not necessarily make money directly from web browsers. First released in 1995, and developed for free inclusion within the Windows 95 operating system, Internet Explorer was an early web browser that helped establish the market dominance of Microsoft. The Safari web browser is also free and comes pre-installed on Apple computers, and is tailored for the Apple 'environment'.

A competitor to Internet Explorer in the PC environment is Firefox. Like most other web browsers, Firefox is available to consumers for free. Mozilla, who provides Firefox, had a commercial agreement with Google between 2004 and 2014 in which Google paid Mozilla to be the default search engine on Firefox. Yahoo is now the default search engine on Firefox subject to a similar agreement. [64]

Similar commercial agreements have established Google as the default search engine in Apple Safari and Opera. Microsoft drives traffic to its own search engine Bing by having it as the default search engine on Internet Explorer. Similarly, Google's Chrome operating system has Google as its default search engine.

The business models that support the distribution of browsers do not appear to depend upon the collection of personal information for behavioural advertising. The information they process tends to be used to support the services they provide.[65] However, browsers can be set up to either block or enable cookies, which are necessary to provide users with behavioural advertising. The default setting in most browsers permit the use of cookies to track users.

The default setting in Apple Safari is more 'privacy-friendly' – it only allows cookies and website data from websites the user visits, which helps to prevent some advertisers from tracking users across websites. Apple Safari users can also opt to always block cookies. Apple's policy towards cookies aligns with a broader policy statement against the commercialisation of users' personal information stored on iPhones or in iCloud.[66] Apple has an advertising program called iAds, but it does not currently support that platform with the in-depth user information that it has available to it – a stand that has attracted criticism from advertisers wanting to target customers based on their geography, purchase history, and media interests.[67]

6.1.3. Search engines

[64] Mozilla makes Yahoo the default Firefox search engine in U.S - http://bit.ly/1yUo7Q9
[65] Which browser is better for privacy - http://bit.ly/1eSIqla
[66] Apple privacy - http://apple.co/1RHcreJ
[67] See 'Ad agencies are sad that Apple cares about your privacy' - http://engt.co/1ThJUPg

The global search engine market is dominated by Google. In 2014, Google earned $US 59 billion in online advertising revenue, which accounted for 90 per cent of its total revenue.[68] The reach of Google's advertising depends upon the success of Google as a search engine and the popularity of its other services including Gmail, Google Maps, and Google Plus. Google's success as an advertising platform is strengthened by its ability to collect and process the information of users across its services, enabling advertising based upon the behaviour and interest profiles of users.[69]

Like Google, Yahoo also depends upon advertising for revenue; however, Yahoo's main service is as a news and entertainment site. Its current business model depends upon the ability of Yahoo to draw users to its services, such as news, email and search, and the 'click-through' success of advertising displayed on Yahoo sites. Like Google, Yahoo targets users with advertising that it is intended to align with users' interests.[70] Yahoo is the third largest search engine in the US by query volume; however, its search results have at different times been 'powered' by Bing and Google. Under a deal made with Bing in 2009, Microsoft received 12 per cent of advertising revenue generated by Yahoo Search.

ChaCha is a search engine that was launched in 2006 that answers questions through the use of independent contractors called 'Guides' who are paid per question. ChaCha differentiates itself from other search engines by providing answers to questions that are 'human-guided'. The search engine is monetised through third party advertising.

DuckDuckGo distinguishes itself from other search engines by not tracking or profiling its users and by showing all users the same search results for a given search term. The search engine is monetised through native advertising – that is, advertising that relates to the user's search queries. In late 2014, Apple Safari and Mozilla Firefox made it possible for users to set DuckDuckGo as their default search engine.

6.1.4. Social media

Facebook is the world's largest social media site with over a 1 billion users.[71] The site is monetised entirely by advertising. Facebook users receive targeted advertising from third parties based upon the personal information that users supply in using Facebook. Facebook has been at the centre of a number of privacy controversies due in large part to the volume of information that the website collects and the sensitive nature of much of the information that users supply.[72]

Instagram is a popular free social media service that allows users to share photographs and videos on a number of social media platforms. The company was purchased by Facebook in 2012. The service is not yet available to advertisers and does not provide Facebook with revenue.

---

[68] Advertising revenue for Google - http://bit.ly/2303tOD

[69] For example, 'If Google is free how does it make so much money'- http://bit.ly/1MRINPy

[70] Behavioural FAQs - http://bit.ly/2303H8v

[71] Wikipedia entry for Facebook - http://bit.ly/1NY01eV

[72] For example, 'The Austrian thorn in Facebook's side' - http://onforb.es/1UTLlVc

Snapchat allows users to directly send other 'Snapchatters' photographs, videos and messages. The material that is sent over Snapchat is not stored on the recipient's device and is not available to advertisers. The value of Snapchat to advertisers is in its popularity, and advertisers pay to place their advertising on the Snapchat platform. Snapchat has been the subject of a complaint filed by the Electronic Privacy Information Centre with the Federal Trade Commission. Contrary to Snapchat's claim that photos delivered over the service disappear, concern was raised that they can in fact be retrieved with minimal technical knowledge after the time limit expires.[73]

Twitter is an online social networking service that allows users to send and read short messages called 'tweets'. Twitter makes money from advertising. Advertisers are able to purchase 'promoted tweets' that are relevant to searches made on the Twitter website. Small businesses can use self-service tools to create their own advertising on Twitter.

[73] Wikipedia entry for Snapchat - http://bit.ly/1d80rnc

6.2. Privacy policy comparators

6.2.1. Accessibility / length of privacy policies

The privacy policies in our study varied in length between 995 words and 7396 words, with an average of 3232 words. Based on an average reading speed of 250 words per minute, this would take the average reader about 4 minutes to read the shortest privacy policy, 29 minutes to read the longest, and 13 minutes to read a privacy policy of average length.

An estimation of the length of privacy policies is complicated by the fact that a number of service providers present information relating to privacy in a number of separate documents. Yahoo, for example, has three documents that describe privacy and privacy issues with respect to different aspects of its business. Google, also, has a main privacy policy and additional documents on its advertising practices and use of cookies. The privacy policy of Google applies to all of Google products and services, also known as a 'universal policy', which creates a challenge for a user who wishes to identify how a particular Google service collects and uses personal information. Apple also has a universal privacy policy.

The privacy policies of mobile device apps are available through app store webpages that display apps. The user must click on a graphic depicting an app in order to gain more information about the app, including the licence agreement for the app and the privacy policy. The privacy policies of other sites are generally available as links on download pages or website pages.

6.2.2. Contractual issues

Most of the service providers in this analysis attempt to bind the user to contracts, described variously as terms of service, terms of use or licence agreements. Privacy policies are sometimes treated as binding contractual documents in their own right (for example: Instagram, Supercell and Kabam); other times the primary contract incorporates the privacy policy into the contract (for example: Glu, Instagram and Snapchat). A number of service providers state both in the contract and the privacy policy that use of the service binds the user to the terms of the privacy policy (for example: Twitter).

However, people who use the Firefox browser are subject only to the terms of the Mozilla public licence, and there is no attempt by Mozilla to bind users to its privacy policy. The DuckDuckGo site informs users that they are not subject to any binding contractual terms.

The ordinary mechanism by which users signal their acceptance of these contracts and privacy policies is through the use of services ('browsewrap').

People who use Apple products such as the Safari browser must first accept terms of service by 'clicking' accept ('clickwrap').

A number of service providers – for example Opera, Internet Explorer, Google, Yahoo, Twitter and Facebook – also state in their terms of service and privacy policies that they may update their policies. According to most privacy policies, the user bears the responsibility for checking policies and terms of use from time to time for updates. Typically, the user accepts the changes to privacy

policies by continuing to use the service or product (for example Facebook, Instagram, Twitter and Snapchat).

6.2.3. Self-regulatory schemes

A number of service providers state in their privacy policies that they comply with the standards required to display the TRUSTe privacy seal. This scheme has been the subject of significant criticism with respect to its lack of enforcement actions and with respect to the compliance claims of participants.[74]

A number of US companies also make reference to their participation in the EU-US Safe Harbor scheme. This scheme was declared to be invalid by the European Court of Justice in October 2015.[75]

References in privacy communications to privacy seals and privacy schemes that have been either discredited or invalidated have the potential to mislead consumers about the extent to which service providers adhere to privacy standards.

6.2.4. Security claims

Most service providers make broad claims about their security measures, including physical, business and technical security measures. A number make more specific references to particular practices. With regard to Internet Explorer, Microsoft states 'we store the personal information you provide on PC systems with limited access, which are located in controlled facilities.' Yahoo extends security to internal controls: 'we limit access to personal information about you to employees who we believe reasonably need to come into contact with that information to provide products and services to you or in order to do their jobs.' A number of other service providers make reference to their use of encryption technologies such as SSL to store sensitive personal information (for example Kabam and Tencent). Google also states that it encrypts many of its services using SSL.

Mozilla, which provides the browser Firefox, is the only service provider that states that it will notify users where they learn of a security breach.

6.2.5. What information is collected?

Much of the material within privacy policies is dedicated to descriptions regarding the collection by service providers of different types of information about consumers, how that information is collected, and the purposes to which that information is put. This information is largely anonymous and may or may not be 'personal information' under the Privacy Act depending upon whether it can be regarded to be 'reasonably identifiable' in the circumstances (see also 4.3.1 Definition of 'personal information') . The descriptions of types of information collected contribute significantly to the length of privacy policies and are likely to also contribute significantly to the perception that they are complicated.

The types of information collected can be included within broad categories that reflect how information about consumers is collected. The categories considered in this study are:

[74] Galexia Consulting report, The US Safe Harbor – Fact or Fiction (2008)

[75] Europe's top court strikes down safe harbour data transfer agreement - http://tcrn.ch/1OUYEBw

- User supplied data
- Device data
- Use data
- Cookie tracking data
- Search data
- Data collected from third parties
- Information collected by third parties for behavioural advertising
- Non-personally identifiable information.

User supplied data refers to personal information that the consumer provides. This information may be supplied as a result of surveys, competitions, social media messages, or through registration, and is likely to include information such as name, contact number and email address. While the consumer is likely to be aware of the collection of personal information, the consumer does not necessarily understand how the information will be subsequently used and disclosed.

Device data is information that relates to a user's phone, tablet or desktop computer. All devices that connect to the internet provide packages of information that enable the device to be recognised and included on a network. Device data is collected automatically and the ordinary consumer is unlikely to be aware of its collection. This data includes information that helps to identify a device, such as IP address, MAC address and unique device ID. Device data is generally 'functional' in the sense that is vital to the basic architecture of the internet. While device data has a functional purpose, it is nevertheless personal information if it can be linked to an identifiable person.

Use data, which is sometimes referred to as log data, is information automatically recorded when a particular device accesses a particular site. Use data allows traffic on the internet to be measured and analysed, and has functional importance.

Cookie tracking data is data generated by cookies placed on users' devices that enable service providers to track the online behaviour of users across multiple websites. This data is frequently used to provide information relating to a particular device that can be used for online behavioural advertising.

Search data or *query data* is a record of a user's search inquiries made on search engines. This information is collected and used by search engines such as Google, Yahoo! and ChaCha, and is used to generate behavioural advertising. DuckDuckGo claims to save searches, but not in a way that they can identify the user. The consumer plays a part in generating search data; however, it seems likely that the extent of the awareness of the consumer that this information is collected and processed to produce behavioural advertising depends upon the consumer and her level of background knowledge.

Data collected from third parties is information about a user that is not collected directly from the individual but from a third party. This information is used by the service provider to help form a profile of the user and to provide the user with behavioural advertising.

Information collected by third parties for behavioural advertising is information that the service provider makes accessible through its website and that is disclosed to third parties in order to provide consumers with behavioural advertising. The third party collection of information for behavioural advertising represents a challenge for consent because in entering a relationship with a first party service provider the consumer is positioned to provide consent or contractual acceptance to the first party, not to third parties.

Non-personally identifiable information is information that the service provider claims is not subject to the same requirements as identifiable information because of its anonymity. Mozilla, Apple, ChaCha and Yahoo! make claims with respect to this type of information; however, the claim is open to criticism unless a service provider can demonstrate that this type of information is genuinely incapable of identifying an individual.[76]

[76] This issue is discussed at length in the 2012 FTC report, see note 34, pp18-19.

6.2.6. Purpose of collection of personal information

The purpose for which personal information is collected is 'suggested' to some extent by the category of information that is collected: for example, *device data* identifies devices, *use data* provides information about when particular devices connect to particular websites, and *user supplied information* is sometimes collected simply as a means by which service providers can contact users.

However, understanding the purpose of the collection of information is far from straightforward. Service providers collect sets of information relating to individuals via multiple means and sources, and use that information for multiple purposes.

The APPs and similar examples of information privacy principles are based upon a simple model of information collection in which a single entity directly collects a single set of personal information to be used for a specific purpose. The simplicity of this model permits transparency – the individual knows *who* has collected personal information, *how* it has been collected, and *what* it is to be used for. However, current practices allow multiple collectors of personal information, multiple means of collection and multiple purposes.

The fact that there are multiple collectors of personal information means that a consumer may be required to read more than one privacy policy if she wants to inform herself about how her personal information will be handled. This is either unreasonable (because the consumer should only have to read one privacy communication), impracticable (because it would take a consumer a long time to find all the relevant privacy policies) or impossible (because the service provider does not list all the third party recipients).

Descriptions of the purposes of collecting information could be simplified for consumers through the use of clearer categories of purpose. In particular, technical, functional and administrative uses of information should be distinguished from marketing and commercial uses on the grounds that these latter uses may be more relevant to the privacy interests of the consumer.

6.2.7. Treatment of third party issues

The collection of personal information by third parties creates a number of possible problems for privacy protection, consumer consent and contractual fairness: it expands the number of entities that can hold and use a consumer's personal information; it undermines the principle that a contract binds two parties only and does not include external parties; and places a burden on consumers to read third parties' privacy policies.

A review of privacy policies reveals that service providers adopt a number of different approaches to third party issues. A number of service providers (for example Supercell, Kabam, Apple and Google) state that third-party collection of personal information is subject to the third party's privacy policy. Glu goes further by stating that it takes no responsibility for the use of third-party tracking technologies.

On the other hand, Tencent states that it uses reasonable efforts to ensure that third parties comply with Tencent's privacy policy. The Firefox privacy policy goes further and states that third parties are contractually obligated to handle personal information in a way approved by Mozilla. The Internet Explorer privacy policy indicates that it will not transfer a consumer's personal information to third parties without the consumer's consent. DuckDuckGo states that third parties do not receive personal information.

6.2.8. Data Retention

There is no specific requirement under law for service providers to delete the personal information at a specific time; however, it seems reasonable for service providers to delete personal information when it is no longer needed for the purpose for which it was originally collected.

Most service providers are not very clear about when they will delete personal information: they either provide no information (for example Apple Safari, Google, Glu and Yahoo!) or they indicate that personal information will be kept indefinitely. The Facebook privacy policy states that personal information will be kept 'as long as it is necessary to provide products and services to [the user] and others.' The Instagram privacy policy states that when a user terminates an account, their personal information will be kept 'for a commercially reasonable time for backup, archival and/or audit purposes.'

The Firefox policy, on the other hand, states emphatically that 'we don't want your personal information for any longer than we need it, so we only keep it long enough to do what we collected it for. Once we don't need it, we take steps to destroy it unless we are required by law to keep it longer.'

The Twitter policy states that Twitter deletes 'log data' (also known as use data) after a maximum of 18 months.

6.2.9. Overseas Transfers

Communications sector service providers operate in international markets; however, they also have obligations under a number of domestic jurisdictions, including Australia's, with regard to the transfer of personal information overseas. While some service providers are silent on the issue of overseas transfers of personal information, a number inform the consumer that their servers may operate in jurisdictions other than their own. Tencent, for example, states that they 'operate and may continue to operate servers in a number of jurisdictions around the world, so the server on which your personal information is used may not be in your jurisdiction.'

A number of entities go further and state that users 'consent' to the transfer of personal information overseas. It is questionable whether a user can provide consent to a term in a privacy policy unless the existence of the term is specifically brought to the user's attention.

6.3. Additional considerations

6.3.1. Meeting communications challenges

Technical language

The language used in the privacy policies examined did not appear to the project staff to be overly technical. By the same token, it seems likely that the level of background knowledge of the consumer will have a significant impact on the extent to which the language used by service providers seems technical.

Legal language

The language used in the privacy policies did not appear to the authors to be overly legalistic. Some privacy policies appeared to be drafted in plain language – for example those of Google and Mozilla. However, the effective communication of legal issues involves more than the presentation of terms in plain language, and it is open to question how well the average consumer would interpret the legal aspects of privacy policies.

Lack of balance in description of practices

The main communication challenge to the drafters of privacy policies appears to be how to convey complex information to consumers with accuracy and clarity, in a way that is easy to understand.

In making this point, it is also necessary to give consideration to the fact that it is not just the accuracy and clarity of information that is important, but also the extent to which the information is likely to be of interest and relevance to people. The bulk of the information in the privacy policies reviewed in this project describes technical, functional and administrative uses of personal information that has value in its own right, but which is unlikely to be of direct interest to most consumers.

The inclusion of too much information about technical, functional and administrative uses of personal information is likely to create in consumers the impression that the use of personal information is essentially non-commercial.

The fact that, in many cases, the primary *commercial* purpose for collecting and using personal information is to create revenue through behavioural advertising is a point that is not adequately highlighted in any of the privacy policies reviewed.

The lack of emphasis on this important point may be regarded as evidence of a lack of neutrality in the manner which privacy information is communicated to consumers. This lack of neutrality is also evident in the different ways in which privacy policies describe the practice of behavioural advertising. For example, the Supercell privacy policy states 'These [third party] advertisers may use information about your visits to our Service… to provide advertisements about goods and services of interest to you.' This description of the practice appears to over-emphasise the benefit to consumers of behavioural advertising and under-emphasise the possible privacy implications.

Use of the word 'may'

A number of privacy policies use language that fails to pinpoint precisely what the service provider does, which is likely to confuse readers and leave them with a sense of uncertainty. This is true where the modal verb 'may' is used to describe what service providers do.[77] For example, the Apple Privacy Policy states 'We **may** collect and store details of how you use our services, including search queries. This information **may** be used to improve the relevancy of results provided by our services.

[77] See also A Gniewek, 'Google Privacy Policy – 'In Breach of EU Law?'', 7(2) Masaryk University Journal of Law and Technology.

Except in limited instances, to ensure the quality of our services over the Internet, such information will not be associated with your IP address'.[78]

It is more helpful to a consumer where a service provider describes exactly what the service provider does in certain circumstances.

The use of the word 'may' is particularly prevalent in the Google and Apple privacy policies (33 and 44 uses respectively), which is likely to reflect the fact that these are universal policies that apply across all of Google's and Apple's services.

The use of the term 'may' is also problematic for consumers because it appears to give the service provider 'permission' to perform certain practices that it does not yet do, without specifying whether the service provider currently does or intends to do the activity.

[78] Apple Privacy Policy (emphasis added).

Apple Privacy Policy

Collection and Use of Non-Personal Information

We also collect data in a form that does not, on its own, permit direct association with any specific individual. We **may** collect, use, transfer and disclose non-personal information for any purpose. The following are some examples of non-personal information that we collect and how we **may** use it:

- We **may** collect information such as occupation, language, postcode, area code, unique device identifier, referrer URL, location and the time zone where an Apple product is used, so that we can better understand customer behaviour and improve our products, services and advertising.
- We **may** collect information regarding customer activities on our website, iCloud services and iTunes Store, and from our other products and services. This information is aggregated and used to help us provide more useful information to our customers, and to understand which parts of our website, products and services are of most interest. Aggregated data is considered non-personal information for the purposes of this Privacy Policy.
- We **may** collect and store details of how you use our services, including search queries. This information **may** be used to improve the relevancy of results provided by our services. Except in limited instances, to ensure the quality of our services over the Internet, such information will not be associated with your IP address.

Google Privacy Policy

How we use information that we collect

We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones and to protect Google and our users. We also use this information to offer you tailored content – like giving you more relevant search results and ads.

We **may** use the name that you provide for your Google Profile across all of the services we offer that require a Google Account. In addition, we may replace past names associated with your Google Account, so that you are represented consistently across all our services. If other users already have your email or other information that identifies you, we may show them your publicly visible Google Profile information, such as your name and photo.

…

We **may** combine personal information from one service with information, including personal information, from other Google services – for example, to make it easier to share things with people you know. We will not combine DoubleClick cookie information with personally identifiable information unless we have your opt-in consent.

…

Google processes personal information on our servers in many countries around the world. We **may** process your personal information on a server located outside the country where you live.

7. Consent and Consumer Empowerment

A vital aspect of communication with consumers concerns the manner in which consumers provide consent for the collection and use of their personal information. This is a communication issue as well as a legal issue because the quality of communication with respect to the formation and content of agreements with consumers is important for the validity and fairness of those contracts, and the extent to which the consumer can be regarded to have given consent for the collection and use of personal information.

Improving the communications and interactions with consumers is likely to require a dynamic, iterative process in which service providers innovate their communications with consumers and extend to them greater levels of control.

Information about a service provider's privacy practices is more interesting and relevant to a consumer where that information provides the consumer with the ability to exercise control over her personal information. From the consumer perspective, providing the consumer with options is likely to make the consumer feel that she is participating and engaging in the relationship with the service provider, as opposed to passively acquiescing to whatever practices are being described within privacy policies.

In turn, a higher level of participation and engagement by the consumer is likely to improve the extent to which the consumer takes an interest in privacy information. With the ability to exercise choice, the consumer is asked to turn her mind to those options that represent her best interests.

In terms of the *cost* of reading privacy information, the inclusion of privacy options alongside privacy information provides an incentive for consumers to read. A 'take it or leave it contract' only provides a net benefit to the reader where the reader decides on balance to walk away from it. Where the consumer has already decided to acquire or use a particular product or service, the consumer has little reason to read privacy information that cannot be acted upon.

7.1. Consent in the Privacy Act

Subject to exceptions, APP entities are not required under the Privacy Act to receive the formal consent of individuals before collecting personal information. One exception is where an entity collects sensitive personal information (APP 3.3). Consent is also sometimes required from individuals before entities are able to use personal information for a secondary purpose (APP 6.1) or when personal information is disclosed overseas (APP 8). Individuals are also able to 'opt out' from having their personal information used for direct marketing purposes. While the failure to opt out is

unlikely to be regarded as true or legitimate consent,[79] nevertheless the ability to opt out provides consumers with a level of control over how their personal information is used.

Despite the fact that entities are not required under the Act to receive the consent of consumers before collecting personal information, the requirement for entities to have privacy policies and to provide consumers with notices regarding the collection of personal information indicates that consumers have rights to receive information about privacy and, presumably, to act upon that information – for instance, by refusing to accept the contract.

The ability of a consumer to accept or reject a contract is a basic means by which the consumer is able to exercise consent with respect to the terms and conditions of a contract. This approach to consumer privacy protection has been dubbed 'notice and consent' in the United States and has been criticised because of the lack of privacy protection it affords consumers who do not read or understand consumer contracts.[80] In Australia, however, consumers have the safety net of the Australian Privacy Principles which provide some protection of consumers' interests in the absence of informed consent.

7.2. Contractual acceptance versus consent

The concept of consent should be distinguished from the concept of acceptance in contract. Standard form contracts in which acceptance is signalled through use of a product or service (often referred to as 'browsewrap' in the context of websites) enable consumers to be bound to the terms of a contract without the consumer having knowledge of the terms. The concept of consent, as it is normally understood, requires the consumer to have a basic level of awareness of the subject matter to which he is giving consent.

A number of consumer contracts and privacy policies examined in this study state that a consumer accepts the service provider's privacy policy by using their service. These 'browsewrap' contracts appear to indicate that the consumer provides acceptance under contract law for contractual terms and conditions; however, these contracts should not be regarded as indicating that the consumer provides genuine, informed consent for the collection and use of personal information (see also 6.2.2 Contractual issues and 8. Contract and consumer law).

7.3. The meaning of consent

At its strongest, consent refers to the explicit informed consent of the individual – a form of consent that reflects the genuine acceptance of the individual to something based upon a proper understanding of what it is the individual is consenting to.

Legal academic Margaret Jane Radin defines 'free consent' as something that requires 'a knowing understanding of what one is doing in a context in which it is actually possible for one to do

[79] See Australian Privacy Principles guidelines see note 4, pp 8-9.
[80] Nissenbaum, see note 6.

otherwise, and an affirmative action in doing something, rather than a merely passive acquiescence in accepting something.'[81]

There are three elements in Radin's definition which can be categorised as 'being informed', 'having alternatives' and 'active acceptance'. These categories are echoed by the OAIC Australian Privacy Principles guidelines (2014)('OAIC guidelines') which states four key elements of consent:

- The individual is adequately informed before giving consent
- The individual gives consent voluntarily
- The consent is current and specific
- The individual has the capacity to understand and communicate their consent.[82]

The Privacy Act does not define 'consent', other than by stating that consent is either express or implied.[83] What constitutes consent is a vexed question to which there is no clear academic or legal consensus. A possible reason for the confusion is the fact that consent concerns two interrelated concepts: the mechanism that the consent-giver engages with in order to indicate that the consent-requester is permitted to perform particular actions ('technical consent'); and the informed, free intentions of the individual ('true consent').

Technical consent can be indicated in an objective way – for example, by clicking a box that demonstrates an individual's agreement. A user either clicks the box or does not.

True consent, however, is a nuanced concept that relates to the individual's understanding of her own awareness, intentions and sense of autonomy. True consent does not provide a practical mechanism by which to demonstrate its existence. Reliance upon a technical mechanism for showing consent seems to imply that the accepted standard of consent will always be less than true consent.

Viewed pragmatically, service providers should not be held to a standard of true consent. The standard to which service providers should be held should relate to the *opportunity* they present consumers with to provide consent that is informed and voluntary.

From this standpoint, the consumer bears some responsibility to inform himself and to turn his mind to the terms and conditions for which consent is being requested.[84] However, the level of effort that can reasonably be expected of consumers in informing themselves is a question to which there is no easy answer.

This research proposes that the question of consent is a matter of balance. In most situations, consent is unlikely to be true or free in the strictest sense because it can never be based upon

[81] M Radin, *Boilerplate: the Fine Print, Vanishing Right, and the Rule of Law* (2013), p1126.
[82] See note 4, pp8-10.
[83] *Privacy Act 1988* (Cth), sect 6.
[84] See ACMA research see note 56, p3.

perfect knowledge of the consequences of providing or withholding consent. The most that can be asked is that consent is 'good enough'.

How consumers make decisions based upon limited information, and with limited time and attention, is a question that has received a lot of attention in the field of behavioural economics. This means of examining, researching and testing consumer behaviour represents a rich opportunity for an improvement in how information is presented to consumers, and how the presentation of information affects the choices consumers make.

7.4. Differences between consent and contractual acceptance

A consumer can signal acceptance to a contract in circumstances in which it seems unlikely that the consumer understands the consequences of her actions (see 8.4 New environment). The fact that the law permits this deserves attention. While an argument may support the legal recognition of clickwrap and browsewrap contracts on the basis of economic efficiency where the contract terms are reasonable, it is questionable whether this argument is convincing when extended to terms relating to the collection and use of consumers' personal information. It is necessary to draw a sharp distinction between acceptance of contract and the giving of consent.

Consent also seems to be distinguishable from acceptance in contract on the basis that it does not bind the consent-giver in the same way and to the same extent as contract. According to the OAIC guidelines, consent cannot be assumed to endure indefinitely.[85] The guidelines also state that an individual may withdraw consent at any time.[86] If this is true, then consent is clearly a different concept from that of contractual acceptance.

However, a question remains with regard to whether an individual can withdraw consent in circumstances governed by contract. Where both contract and consent apply to a permission granted by an individual, is it enough for an individual to withdraw consent in order to end the permission? A privacy framework based upon consent may also have to shape the elements that are permissible in contract.

7.5. Framing effects and consent

The framing effect is an aspect of behavioural economics that describes how the *presentation* of options – not the *substance* of options – impacts upon the choices individuals make.[87] The size of the effect relates to whether or not options are perceived as losses or gains. Prospect theory, which is the central theory behind the field of behavioural economics, contrasts with the 'rational actor model' of classical economics theory in which the presentation of information is considered to be irrelevant.

[85] See note 4, p10: 'Consent given at a particular time in particular circumstances cannot be assumed to endure indefinitely. It is good practice to inform the individual of the period for which the consent will be relied on in the absence of a material change of circumstances.'
[86] See note 4, p10.
[87] See note 4, p10.

The impact of framing effects has been considered in the context of privacy policies. A 2013 Korean study compared the differences in outcome depending upon whether people are asked to either opt in or opt out with regard to a practice that appears to reduce the individual's level of privacy.[88] In the study, the consequences of the consent requests are identical – the only difference is the method of seeking consent. The study found that overall, across 17 common categories of personal information, that people are more likely to protect personal information where it is provided by opting in (72 per cent) than where protection of personal information is maintained by opting out (46 per cent).

The framing effects between opt in and opt out were found to be small in relation to the protection of highly sensitive personal information such as social security number (92 per cent versus 95 per cent). The reason for the lack of a framing effect here appears to be due to the fact that the collection of information perceived as sensitive or risky encourages the individual to take the active step of opting out.

A significant difference between the two methods of seeking consent was observed where the permission related to personal information that was perceived as having a lower risk. With opt-in leading to a greater willingness to protect personal information, the study found the following differences between opt-in and opt-out for the collection of certain types of information: gender (15 per cent), email address (20 per cent), age (20 per cent), address (24 per cent), hobby (38 per cent), and religious opinion (57 per cent).[89]

An ACMA study on informed consent supported the view that the perception of risk – whether the risk related to privacy, finances or the reputation of a company – also has an impact on the preparedness of consumers to take steps in informing themselves about the terms of contracts.[90]

The difference between opt-in and opt-out is an important consideration with respect to APP7 (direct marketing), because of the way in which it distinguishes between direct marketing entities that require opt-in consent and those that require opt-out consent.

7.6. Improving the standard of consent

The standard for consent in consumer affairs is not well-developed or accepted and there is no consistent guidance to industry on requirements for consent.[91] Among the relevant industry codes,

[88] Y Baek, Y Bae, I Jeong, E Kim and J Rhee, 'Changing the default setting for privacy protection: What and whose personal information can be better protected?'(2014), 51 Social Science Journal, pp524-33.
[89] See above, p529
[90] See note 56, p3.
[91] See for example Australian Communications Consumer Action Network, Informed Consent Research Report, p6:
'The collection of informed consent from consumers is a key requirement in the communications sector. It is essential for contract formation, subscription services and use of customer information. However, there is no single location for a definition of consent – and consent requirements are scattered throughout a mix of common law, generic consumer laws, specific telecommunications laws and industry codes of conduct.'

the Telecommunications Consumer Protections Code is notable for requiring a supplier to take all reasonable steps to ensure that the consent of the consumer is informed consent.[92]

There are particular elements connected to the provision of consent that when improved are likely to improve the standard or quality of consent provided by the consumer. That is, the consent is more likely to align with the voluntary, informed intentions of the consumer. These elements apply equally to the circumstances in which a consumer accepts the terms of a contract.

This research identifies and focuses on the following elements of consent and their connection to the quality of consent:

- Intentionality
- Reasonableness
- Certainty and specificity
- Quality of communication.

7.6.1. Intentionality

Intentionality relates to the extent to which the consent provided by the consumer is free and unencumbered. The intentions of the consumer are best provided for by allowing consumers to make decisions in circumstances that do not unfairly influence the decision of the consumer. The standard of intentionality is influenced by a number of factors including voluntariness, whether consent is express or implied, whether consent is attached to single requests or is bundled, the likely cognitive limitations of the consumer, and the timing of the request for consent.

Voluntariness

Consent should be voluntary; however, some contexts in which consent is given may be regarded as being more voluntary than others. The OAIC guidelines state that the question of whether consent is voluntary is influenced by the extent to which the consumer has viable alternatives and the seriousness of consequences of withholding consent.[93]

Express consent

The concept of intentionality relates to what the consumer believes she has agreed to. It incorporates the entire scope of the consumer's awareness with respect to her relationship with an entity, including the question of whether she believes she has given consent to an entity and what the implications are of having given consent.

Consent is 'stronger' where a consumer provides express consent as opposed to implied consent. The intention to provide consent is more clearly demonstrated where consent is express. Consent is stronger still where the consumer has a good understanding of the consequences of providing consent.

[92] Telecommunications Consumer Protections (TCP) Code (2012), sect 7.3.
[93] See note 4, p9.

In order for consent to be successfully implied a party must show that consent can 'reasonably be inferred in the circumstances'.[94] It is questionable whether a mere failure to opt out implies that an individual indicates consent.[95] Where entities rely upon implied consent, implied consent is likely to be stronger where the consumer is provided with a prominent option to opt-out, and where the consequences of failing to opt out are not serious.[96]

The implications of bundled consent

The intention of the consumer is also likely to be undermined by the bundling of consent – a practice in which a consumer is asked to provide a single consent with respect to multiple requests. Where consent is bundled, the consumer must withhold consent for all requests in order to withhold consent to just one request. In such a situation, a consumer is likely to feel pressured to provide overall consent, despite being unhappy about one or more particular requests. The problem of bundling is also evident where consumers are required to accept the terms of a consumer contract and, in doing so, also accept the terms of a privacy policy.

The impact of bundling consent on consumers' decisions to give or withhold consent is capable of being measured by fieldwork.

Cognitive limitations and understanding consequences

A number of commentators argue that in order for consent to be meaningful that it is necessary for consumers to understand the trade-offs.[97] The negative consequences of providing consent have to be capable of being accurately compared to the apparent benefits of providing consent.

The negative consequences relate to long term privacy concerns, whereas the benefits relate to short term gains. In order for a consumer to develop an understanding of long term interests, it is necessary for the consumer to have a good 'view of the whole'. The concern expressed by Sloan and Warner is that the process by which consumers incrementally trade privacy for short term gains – such as the use of an internet service or an app – can undermine privacy in a way the consumer would be unlikely to agree to if the consumer had a good appreciation of the long term risks.

The ability of the consumer to assess risk is also affected by a cognitive bias – another aspect of prospect theory – in which individuals tend to place too much emphasis on short term risks and benefits compared to long term risks and benefits.[98]

---

[94] See note 4, p8.

[95] See note 4, p8.

[96] See note 4, p8.

[97] See, in particular, R Sloan and R Warner, see note 6. See also, Solove and Nissenbaum, see note 6.

[98] This cognitive bias, known as hyperbolic discounting, is discussed by Xavier, see note 50, p15: 'consumers… tend to be short-sighted when making decisions where immediate costs or benefits need to be weighed against future costs or benefits. For example, consumers may enter long-term telecommunication contracts because they place more value on the immediate benefits of the offer, such as a heavily subsidised

Timing of consent request

The intention of the individual to provide consent is more convincing where the request for consent relates to future acts of the consent requester and the individual has sufficient opportunity to consider the merits of the request. Where consent is requested for actions that have already taken place, the individual is likely to feel obligated or pressured to provide consent.

7.6.2. Reasonableness

When consent should be sought

The OECD Guidelines require consent to be provided *where appropriate*.[99] In the Privacy Act, this requirement has been fulfilled by APP 3.3 which obliges entities to obtain the consent of individuals for the collection of sensitive personal information. What constitutes sensitive information is defined by the Privacy Act.[100] Consent is also required in other circumstances in which the individual might reasonably be expect to be consulted – for example, when an entity intends to use personal information for a purpose other than the purpose for which it was originally collected.

Where personal information is to be collected and used in a way that the ordinary consumer is unlikely to expect, there is a greater responsibility on the service provider to present suitable information in relation to the practice and to seek the consent of the consumer. It is also reasonable for consent to be required in relation to practices capable of negatively affecting the individual's interests.

Some practices relating to the collection and use of personal information are likely to be surprising and concerning to many consumers and possibly should require consent, for example:

- Collecting personal information in order to build a profile about an individual
- Collecting personal information in order to make predictions about the individual's habits and interests
- Collecting personal information that is then sold to third parties
- Collecting personal information that is transferred to recipients overseas.

Consent that is unreasonable to request

It should also be contemplated that some requests for consent may be inherently unreasonable. Any request that is likely to have a substantial negative impact on a consumer could be regarded in this light. These requests could be deemed impermissible on the basis that they exploit the uninformed consumer. Conceptualised as an objective standard, there are some requests for consent that the

---

handset, rather than on the long-term costs of being 'locked-in' and unable to switch to access lower-priced alternatives and the latest technology.'

[99] The Collection Limitation Principle states:

'There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge and consent of the data subject.'

[100] *Privacy Act 1988* (Cth), sect 6.

reasonable and informed consumer would not consent to – for example, because the consumer would have to part with his 'immortal soul'.[101]

7.6.3. Certainty and specificity

The standard of consent that a consumer provides can be associated with the certainty and specificity of the terms to which the consumer consents: that is, consent is more meaningful where the consumer has a clear understanding of what it is she has consented to.

With respect to consent, certainty and specificity relate to the *factual elements* and the *duration* of the request.

Factual elements

The proposition that the individual provides genuine consent is strengthened where factual elements are clearly stated within privacy communications. To state the converse, it is unconvincing to argue that an individual provides genuine consent with respect to facts that are ill-defined. While the Privacy Act does not specifically require individuals to provide consent for the collection of personal information, transparency regarding the purpose of collection enables consumers to act upon that information – either by walking away from a contract (if the consumer is not already in one) or by complaining about the purpose of the collection.[102]

The APP guidelines support the idea that the stated purposes of collection of personal information should be specific: 'an entity should not seek a broader consent than is necessary for its purposes, for example, consent for undefined future uses, or consent to 'all legitimate uses or disclosures…'.[103] (See also 6.3.1 Meeting communications challenges).

Duration

The legitimacy of consent is likely to be called into question where consent is provided for an indefinite period of time. Where consent is provided with respect to a limited future use of personal information, a consumer is more likely to understand how personal information is to be used. However, where the use of personal information extends further into the future, a distance is created between the original permission provided by the consumer and the use to which personal information is put. The consumer should be able to withdraw consent for the use of personal information.

7.6.4. Quality of communication

[101] See note 1.

[102] This rationale for requiring the purpose of collection in the APPs is not explicitly stated in the Act. It is implied by the fact that the provision of information about privacy must be of some actionable value for the individual – not just information for its own sake.

[103] See note 4, p10.

Ideally, when a consumer provides consent it is based upon accurate information: that is, consent is informed. However, there is no way to ensure that consumers take advantage of information in order to inform themselves before providing their consent. The best an entity can reasonably be asked to do is to provide consumers with information in such a way as to maximise the likelihood that consumers will inform themselves adequately before providing consent.

The opportunity for informed consent improves with the 'quality of communication' – an expression used here to refer to both the presentation and content of privacy information. Aspects of quality of communication are investigated in 5. Issues relevant to the communication of privacy information.

In summary, quality of communication is affected by:

- The extent to which important or relevant information is brought to the consumer's attention
- The readability of the information and how readers are likely to understand the information based upon their background knowledge
- The level of innovation in the communication of information – how the service provider seeks the engagement of the consumer
- The actionability of the information – the extent to which the information enables consumers to exercise privacy preferences
- The consumer's likely awareness of important legal issues – such as the fact that a service provider is asserting the existence of a contract
- The complexity of the language used to express the information
- The appearance of the information – for example, the size of the font
- The availability of the information in different languages
- How long or concise the communication is.

7.7. Consent and empowerment

The manner in which consumers provide consent for the collection and use of their personal information can be looked at from two perspectives:

- the technical and legal requirements that indicate the consent has legitimately and validly been provided;
- consent that is consistent with more meaningful consumer engagement and participation in relationships with consumers with respect to personal information.

Typically, consent is provided, or not provided, by consumers in response to requests made by entities. In the context of consumer interactions, it is one-sided activity – the consumer has no ability to make similar requests to entities.

The ability of the consumer to provide consent does not, of itself, necessarily provide the consumer with much control over personal information or a high level of empowerment. The extent to which a request for consent has an impact on the level of control the individual has depends upon the circumstances in which consent is requested and the content of the request.

Where the Australian Privacy Principles require consent, it is often in relation to practices that weaken the consumer's level of privacy, for example because it permits an entity to use personal information for another purpose or to send personal information overseas. By refusing consent, the consumer remains in the same position with respect to privacy protection as he would have been had a request for consent never been made.

In order for entities to demonstrate genuine commitment to consumer consent and control, it would be necessary for them to provide consumers with options to control and protect personal information with regard to particular practices such as sharing personal information with third parties and allowing the use of personal information for behavioural advertising.[104]

According to a 2007 US study, the psychology of empowerment is based on four components: meaning, competence, self-determination and impact.[105] The four components are argued to combine to create an overall construct of psychological empowerment. *Meaning* is the value of a work goal or purpose, judged in relation to an individual's own standards or ideals. *Competence* is an individual's belief in his or her ability to perform activities with skill. *Self-determination* is an individual's perception of having choice in initiating and regulating actions. *Impact* is the degree to which individuals believe they can influence outcomes.

7.7.1. Consumer perceptions and trust

The relationship between consumers and entities relies significantly on the trust of the consumer. Consumer trust is important for entities for a number of related reasons, particularly in the e-commerce environment.[106]

The trust of consumers and privacy concerns exist in a dynamic relationship: that is, the trust of the consumer can lessen privacy concerns, and a reduction in privacy concerns can improve trust.[107]

Given the complexity of practices relating to privacy, and the lack of knowledge among consumers, it seems likely that consumers must rely on the perception of trustworthiness – in the absence of genuine knowledge and understanding – in consenting to the privacy practices of entities. The role of trust in lowering concerns about privacy makes it important for entities to understand ways to improve the trust of consumers.

The perception of trustworthiness can be improved through simple 'visual' measures such as having a prominently displayed privacy policy, having 'third party' certifications such as WebTrust and BBBOnline, and the inclusion of an icon to denote secure encryption.[108]

[104] These privacy options were identified by the ADMA report as best practice initiatives, see note 53, p4.
[105] T Van Dyke, V Midha and H Nemati, 'Effect of consumer privacy empowerment on trust and privacy concerns in e-commerce' (2007), 17 *Electronic Markets*.
[106] See, for example, note 105.
[107] See, for example, note 105.

Trust is also improved through consumer empowerment.[109] Providing consumers with privacy options not only improves consumers' protection of privacy, but raises the level of trust the consumer has in a service provider and lowers the level of concern the consumer has with respect to privacy.

Policy options for improving consent and informed decision-making

1. To improve the level of consumer control and the protection of privacy, the range of practices that require consumer consent should be expanded and awareness of those controls should be improved
    - Service providers should avoid bundling consent
2. With regard to consent, consumers should be informed, and have choices and controls with respect to information that they are likely to find important, in particular:
    - The sale of their information
    - The aggregation of their information
    - The analysis of their information
3. Default settings should favour the privacy of the consumer
    - Fieldwork research should provide data with respect to the differences between methods of obtaining consent (eg opt-in versus opt-out)
4. Service providers should maximise the opportunity for consumers to provide informed consent
5. The giving of consent should be separated from any browsewrap and clickwrap contracts
6. Consumers should be able to withdraw consent for the use of their personal information
7. Consumers should be provided with effective notice and privacy controls where service providers change their privacy policies.

[108] X Sheng and P Simpson, 'Effects of perceived privacy protection: does reading privacy notices matter?' (2014), 9 *Int. J. Services and Standards*.

[109] See note 105.

8. Contract and Consumer Law

Most online terms of use, and many online privacy policies, purport to create a contractual relationship with each individual user of online services.

The service providers examined in this project adopt three strategies for making privacy terms contractual:

- Contractual terms of use refer to the provisions of a separate privacy policy and purport to 'incorporate' these into the terms;
- Contractual terms of use include provisions dealing with privacy, and which might otherwise be included in a (separate) privacy policy; or
- The privacy policy is itself expressed to include contractual terms, to which the user agrees.

See also 6.2.2 Contractual issues.

To the extent that they are contracts, all of the terms of use and privacy policies reviewed are so-called 'standard form contracts'. They tend to be presented to the consumer on a 'take-it-or-leave-it' basis, with no opportunity to negotiate terms.

Equally (and once again, to the extent that they are contracts), the terms of use and privacy policies described in Appendix A – Privacy policy comparative analysis table are 'browsewrap' contracts, meaning that the user's assent to terms is expressed to occur upon the doing of a particular act – usually, the continued use of the website or website services.

As discussed below, these forms of contract pose particular challenges to traditional contract theory, which relies on the notion that each party to a contract freely enters the agreement and has the ability to bargain in their own best interests.

To the extent that privacy policies are contractual in nature, this departure from the traditional contractual model also implicates the quality of consent provided from a privacy perspective.

In this section, we consider traditional contractual theory and principles, consumer laws, and their application to online terms of use and privacy policies.

We conclude that standard form browsewrap contracts, in particular, raise a number of issues concerning enforceability and fairness. This, in turn, highlights a number of deficiencies in the provision of assent to online terms (including terms in privacy policies).

8.1. Some definitions

A discussion of online contracts cannot proceed without making clear some aspects of terminology. The focus here will be on 'clickwrap', and – more particularly – 'browsewrap' contracts. These are

progressive iterations of the 'shrinkwrap' form of contracting that developed, in the 1980s,[110] in relation to physical items of software (and which will not be discussed here, having largely been superseded[111]).

[110] D Clapperton and S Corones, 'Unfair terms in "clickwrap" and other electronic contracts' (2007) 35 *Australian Business Law Review*, p154

[111] See above.

There exist some differing interpretations of the term 'clickwrap contract'.[112] However, in this report, clickwrap contracts should be understood to mean contracts that present terms to a user electronically.[113] Terms may appear to a user automatically (for example, by way of a pop-up text box), although this will not always be the case. Users are then asked to agree to the terms, manifesting their assent by, for example, electronically ticking an 'I agree' box. On occasion, users will not be able to manifest their assent, or move to the next screen, until they have scrolled to the bottom of the purported contractual terms, having – theoretically – read these.[114]

The terms of a browsewrap contract, by contrast, may never actively be presented to the website user. They may, for example, be made accessible by way of a hyperlink.[115] There is an absence of active assent, and the user is deemed to assent merely by proceeding to use the website (or by some other action).[116]

8.2. A note about choice of law and forum

The online terms of use of international service providers often purport to choose a certain law and 'forum' for resolution of disputes. Examples of 'choice of law' and 'choice of forum' provisions are provided in Appendix B, showing that the laws of the State of California, and Californian jurisdictions, are common selections.

Parties are free to select both the governing law[117] and forum[118] of a contract. Therefore, to the extent that choice of law and forum provisions are validly incorporated into contractual terms of use, and are not unconscionable or unfair, they are likely to be effective.[119]

Notwithstanding this, our consideration here will be of Australian contractual theory and principles and their application to online contracts.

---

[112] Radin suggests that active user assent may not be required by a clickwrap contract: M Radin, 'Humans, Computers, and Binding Commitment' (2000) 75 *Indiana Law Journal* 112 1128-9. Hughes and Oi suggest that 'clickwrap' contracts relate only to the online purchase of software, whilst 'webwrap' contracts, which – the authors suggest – also require active assent, include the terms and conditions of access of a website, or perhaps the terms upon which a product is purchased from a website: Hughes, Gordon and Ian Oi, 'Shrinkwraps, clickwraps and webwraps: The overseas experience' (2005) 79 *Law Institute Journal* 34.

[113] S Blount, 'Click signatures in webpage contracts' (2008) 46 *Law Society Journal*, p72.

[114] Clapperton and Corones, see note 110, p154.

[115] S Blount, see note 113, p72.

[116] Clapperton and Corones, see note 110, p155.

[117] LexisNexis, *Halsbury's Laws of Australia* (at 2 June 2010) 85 Conflict of Laws, '2 Choice of Law' [85-1180].

[118] LexisNexis, *Halsbury's Laws of Australia* (at 2 June 2010) 85 Conflict of Laws, '1 Conflict of Laws in General' [85-255].

[119] 'However, an Australian court will not give effect to a choice of law made in order to evade the application of a law which would have applied in the absence of such choice if that is a law of the forum': LexisNexis, Halsbury's Laws of Australia (at 2 June 2010) 85 Conflict of Laws, '2 Choice of Law' [85-1180].

Much of the litigation in this area has been conducted in North America (in particular, the United States), and the principles developed there are likely to provide guidance to Australian courts considering similar issues.[120] However, the US environment is to some extent distinguishable from the Australian context, and, where relevant, we will note the differences between the jurisdictions.

Whilst international service providers may effectively 'contract out' of Australian contractual principles, through choice of law and forum clauses, Australian consumer law will still apply to their conduct, to a large degree. The application of Australian consumer law to international organisations is discussed further, below.

8.3. Traditional contract theory

The traditional contract is one that is a 'freely negotiated bargain between the parties'.[121] This was conceptualised as 'freedom of contract' and was central to laissez-faire market theory in the late 19th century.[122] In this context, courts 'saw their role as being one of enforcing, rather than interfering with, contracts'.[123] This anti-interventionist attitude could be justified on the basis of the human autonomy assumed in the traditional contracting model.

In the bargaining process as conceived, each autonomous actor of full capacity freely engages with the other, and freely negotiates in their own interests.[124] Each contracting party voluntarily assumes rights and obligations under the agreed bargain.[125] The concept of freely-given consent is central and a 'non-consensual contract' is 'oxymoronic'.[126]

The contractual model proposed by traditional contract theory involves 'knowing understanding' of one's actions, a free choice in whether or not to contract (and on what terms), and 'affirmative action in doing something, rather than a merely passive acquiescence in accepting something'.[127] Traditional contract theory relates to the concept of consent discussed in section 7.3 Meaning of Consent.

Another – related – concept central to traditional contract theory is the 'meeting of the minds' that is said to occur when the terms of an offer are accepted. In common law (the law developed in

[120] Hughes and Oi, see note 112. See also S Blount, see note 113, p72.
[121] Clapperton and Corones, see note 110, p153.
[122] L Kornhauser, 'Unconscionability in Standard Forms' (1976) 64 *California Law Review* p1152-3; D Khoury, and Y Yamouni, *Understanding Contract Law* (LexisNexis Butterworths, 8th ed, 2010) p17.
[123] Khoury and Yamouni, see notesee above, p17.
[124] LexisNexis, *Halsbury's Laws of Australia* (at 30 March 2015) 110 Contract, '1 Definition and Nature of Contract' [110-10]. Freedom of contract is a principle said to be 'at the heart of contract law': AG, *Interpreting contracts*.
[125] LexisNexis, Halsbury's Laws of Australia (at 30 March 2015) 110 Contract, '1 Introduction - Contract' [110-10].
[126] M Radin, see note 112, p1153
[127] M Radin, see note 112, p1126.

cases, by judges sitting in courts), it has been said that the 'meeting of the minds' moment creates the 'consensus which is necessary according to the English law … to make a contract'.[128]

However, despite the rhetoric that contract requires free choice and a 'meeting of the minds', courts have always applied an 'objective theory' of contract law, and have never enquired into the subjective intentions of the parties.[129] Courts need enquire only into the objective manifestations of intent to contract. This approach can be discerned in the principle, discussed below in relation to online contracts, that signature of a document containing purported contractual terms binds the signing party[130] - even if, in reality, that party did not intend to enter a contract on those terms. This approach has merit so long as a consumer as a party to a contract turns his minds to the possible consequences of entering a contract. The approach has less merit in an environment in which people rarely read contract terms and therefore do not understand the consequences of entering contracts.

[128] *Carlill v Carbolic Smoke Ball Co* [1893] 1 QB 256, 269.

[129] R Nimmer, 'The Legal Landscape of E-commerce: Redefining Contract Law in an Information Era' (2007) *Journal of Contract Law* 10, p25.

[130] See, generally, *L'Estrange v F Graucob Ltd*[1934] 2 KB 394.

8.4. New environment

The contracting practices of the e-commerce environment give cause to re-consider traditional contract theory. Online contracting 'arguably … often occurs with little regard for [traditional contractual concepts] such as capacity [and] consent'.[131] Thus, online contracts 'raise inherent issues of fairness, and undermine the traditional notion of a contract being a freely negotiated bargain between the parties'.[132]

Yet, arguably, 'offline' standard form contracts undermined traditional contract theory even before the advent of the e-commerce age.[133] As Radin contends, '[e]ven before the digital era, the traditional model of contract-as-consent [became] attenuated in practice. Most run-of-the-mill transactions are governed by terms that receiving parties cannot read or do not care to read'.[134] Inequality of bargaining power is a feature of all contracting between an individual and a corporation or the state.[135]

Further, the 'meeting of the minds' view of contract has long been damaged: as Radin argues, '[t]he idea of voluntary willingness first decayed into consent, then into assent, then into the mere possibility or opportunity for assent, then to merely fictional assent, then to mere efficient rearrangement of entitlements without any consent or assent'.[136]

Therefore, online contracts have perhaps only highlighted an existing 'disjunction between transactional practice and the traditional picture of contract-as-consent'.[137] It may be true that freedom of contract no longer exists in any absolute sense,[138] and traditional contract theory, founded on freely given consent, is now well and truly compromised.

8.5. Traditional contract principles

[131] Mathews-Hunt, K. 'CloudConsumer: contracts, codes & the law' (2015) 31 *Computer Law & Security Review*, 31(4), p460. See also Radin, see note 112, p1126.

[132] See note 110.

[133] Due to the prevalence of standard form contracts, contracting is now frequently on a 'take it or leave it basis', meaning that the traditional contractual notion of 'agreement' has been damaged since the mid-20th century: Khoury and Yamouni, see note 122, p18. In early commentary, standard form contracts 'were thought to have a poor fit with conceptions of volitional consent that underlie the neoclassical basis for enforcement of contracts': Gillette 1. See also L Kornhauser, see note 122, pp1153-4.

[134] Radin, see note 112, p1160.

[135] LexisNexis, Halsbury's Laws of Australia (at 30 March 2015) 110 Contract, '1 Introduction - Contract' [110-25].

[136] M Radin, 'Boilerplate Today: the Rise of Modularity and the Waning of Consent' (2005) 104 Michigan Law Review p1223, p1231. See also note 112.

[137] Radin, see note 112, p1126, p1160.

[138] Khoury and Yamouni, see note 122, p18.

Traditional contract principle is the domain of the 'general law', comprising 'common law' and 'equity' (the latter providing broader concessions to notions of fairness).[139]

With the importation of the English legal system in colonial times,[140] Australia inherited principles of English common law on the formation, interpretation, and enforceability of contracts. Today, there are some statutes[141] with relevance to these matters, yet contract remains largely a creature of the common law and equity.

Common law dictates that essential elements for the formation of a contract are:

- agreement, consisting of:
    - offer (by the 'offeror'); and
    - acceptance (by the 'offeree'); and
- an intention to create legal relations.

Another requirement for the formation of a 'simple' contract is so-called 'consideration'.[142] Consideration is something of value, which is the 'price' paid for a promise under the agreement.[143]

Once a contract is considered to have been formed, there are various factors which might render it unenforceable, or allow the bargain to be avoided. If one or more of these factors applies, either specific contractual terms or the whole of a contract may be found to be void, or 'voidable', by one or other party.

Such factors include:

- incapacity of a party; and
- so-called 'vitiating factors', such as misrepresentation and unconscionable dealing.

Further information on the elements of formation of a contract, and on the factors that may render a contract void or voidable, is provided in Appendix C.

8.6. Application of other laws to contracts

[139] Khoury and Yamouni, see note 122, pp11-12.

[140] Khoury and Yamouni, see note 122, p4.

[141] For example, the *Competition and Consumer Act 2010* (Cth), discussed below.

[142] Khoury and Yamouni, see note 122, pp80-1:
'A second [fundamental principle of the law of England] is that if a person with whom a contract not under seal has been made is to be able to enforce it consideration must have been given by him to the promisor or to some other person at the promisor's request': *Dunlop Pneumatic Tyre Co Ltd v Selfridge & Co Ltd* [1915] AC 847, 853.

[143] 'An act or forbearance of the one party, or the promise thereof, is the price for which the promise of the other is bought, and the promise thus given for value is enforceable'. This statement of Sir Frederick Pollock was approved and adopted by Lord Dunedin in *Dunlop Pneumatic Tyre Co Ltd v Selfridge & Co Ltd* [1915] AC 847 at 855. See also N Seddon and M Ellinghaus, *Cheshire and Fifoot's Law of Contract* (2008), p171; Khoury and Yamouni, see note 122, p79.

Consumers are, to a certain extent, recognised as a special class of person, given that they are 'often in a relatively weak position and lack the ability to protect themselves against dishonesty or exploitative terms'.[144] Accordingly, consumer laws, which 'supplement contract law and in some circumstances override contract law rules',[145] have been enacted to protect consumers from the sometimes harsh consequences of traditional contract principles.

Online contracting is 'the burgeoning consumer law phenomenon of the twenty-first century',[146] and, as discussed below, some consumer laws may have the potential to correct the inequities and deficiencies of online standard form contracts.

Consumer laws that are particularly relevant here include:

- legislation dealing with unconscionable conduct (sections 20 and 21 of the Australian Consumer Law ('ACL'));
- legislation dealing with unfair contract terms (sections 23 to 27 of the ACL);
- legislation dealing with unjust contracts (sections 7 to 9 of the New South Wales *Contracts Review Act 1980*); and
- legislation dealing with misrepresentations and misleading and deceptive conduct (sections 18 and 29 of the ACL).

Further information regarding these legislative provisions is provided in Appendix D.

8.7. Application of traditional contract principles to online contracts

As discussed above, online contracts pose challenges for traditional contract theory. They also 'generate some uncertain legal outcomes',[147] prompting two major questions about the application of traditional contract principles in the online environment:

- Do electronic modes of assent suffice as an equivalent to traditional signatures?
- Are online contracts enforceable?

In the United States, the answer to both of these questions is, most likely, 'yes' – with some qualifications.[148]

First, in the US, as in other 'developed' countries, there is now statute establishing equivalence between digital files and paper files.[149]

[144] Australian Attorney-General information sheet, 'Contract law and consumer law'.
[145] See above.
[146] Mathews-Hunt, see note 131
[147] Hughes and Oi, see note 112.
[148] Nimmer, see note 129, p24.
[149] Nimmer, see note 129, p24.

Secondly, US law has held '[c]lick and other online methods of assent [to] create enforceable contractual obligations if the presentation of the method of assent and accessibility to the contract terms is sufficient to give a reasonable person reason to know that terms are being proposed'.[150] Yet, 'there are serious concerns about [the enforceability of browsewrap contracts], even in the United States'.[151]

In Australia, digital equivalence has also been established by the passage of the Commonwealth, State and Territory Electronic Transactions Acts.[152] These Acts provide generally for the validity of transactions undertaken by way of electronic communication,[153] and specifically state that the formal requirement of a signature is taken to have been met, in relation to an electronic communication, by a method used to identify the relevant person, which indicates that person's intention, and which fulfils certain other criteria.[154]

Yet, in the case of many browsewrap contracts, it may be unclear whether a contract has been formed under Australian law.[155] As appears below, the enforceability of online contracts – particularly, browsewrap contracts – is a highly contextual and unresolved issue under Australian law.

[150] Nimmer, see note 129, p24.

[151] Clapperton and Corones, see note 110, p157.

[152] For example, the *Electronic Transactions Act 2000* (NSW).

[153] See, e.g., s 7 *Electronic Transactions Act 2000* (NSW).

[154] See, e.g., s 9 *Electronic Transactions Act 2000* (NSW).

[155] Attorney-General, *Improving Australia's Law and Justice Framework*, 10.

8.8. Issues arising

8.8.1. Formation: Offer and acceptance

'Web age contracts do not [conform easily to established contractual principles], particularly in regard to offer'.[156]

Standard form terms displayed on a website are likely to be considered an offer to contract (rather than a so-called 'invitation to treat' in response to which an offer is made).[157] Accordingly, once acceptance of the terms occurs (and if there is a sufficient intention to create legal relations), the agreement is concluded.

In the case of a clickwrap contract, acceptance is likely to occur 'when the offeree performs the "last act" of clicking the virtual "OK" button', having been earlier presented with the purported terms.[158] This is the act recognised as equivalent to a written signature.[159]

On traditional principles, it is for the offeror to designate the manner of acceptance.[160] Therefore, in the case of browsewrap contracts, it is theoretically open to a website operator to specify that use of the website will constitute acceptance.

Nonetheless, as will be discussed below, this mode of acceptance raises issues concerning the timing and prominence of notification of terms – to the extent that questions are raised as to enforceability.

8.8.2. Capacity

It may be that many online contracts are entered into by individuals lacking legal capacity to do so. For example, it can be assumed that a large number of online contracts are with minors, and are not for 'necessaries' – goods and services which are deemed necessary or beneficial to them (a factor that generally renders such contracts valid[161]).

However, a party seeking to avoid a contract on the basis of incapacity must be able to prove that the other party knew, or ought to have known, of their condition. And, as recognised in the context of unconscionable dealing (which raises similar problems, as discussed below), '[a]n electronic contract is rarely entered into in circumstances where [the website operator, or supplier] has the opportunity to observe the physical or constitutional weaknesses of [the user]'.

---

[156] S Blount, *Electronic Contracts: Principles from the Common Law* (LexisNexis Butterworths, 2009), p41.
[157] Blount, see note 156, p42; see also Hughes and Oi, see note 112.
[158] Blount, see note 156, p42; see also *eBay International AG v Creative Festival Entertainment Pty Ltd* (2006) 170 FCR 450, 464.
[159] *eBay International AG v Creative Festival Entertainment Pty Ltd* (2006) 170 FCR 450, 464.
[160] Hughes and Oi, see note 112.
[161] Khoury and Yamouni, see note 122, p240.

Therefore, it will likely be difficult for the individual user of a website to avoid an online contract on the basis of incapacity. An exception to this principle might arise where website users are asked to verify their age to gain access, and truthfully do so (revealing that they are minors).

Nonetheless, the quality of consent that may be provided by a person lacking legal capacity to contract is a factor that should be considered in determining future policy on online contracts.

8.8.3. Incorporation of terms

Case law and principle suggest that all of the written terms contained in an online contract are likely to be incorporated by electronic signature. In other words, the terms of a clickwrap contract – to which a user has assented, by way of an electronic action – are likely to be enforceable in Australia, whether or not the user has read those terms.[162]

Whilst, in reality, online standard form contracts challenge the consensual 'meeting of the minds' view of contract,[163] 'the [current] rule is that in the absence of fraud or other special circumstances, an electronic signature adopts all the terms of a contract, whether or not the person signing knows the terms of the contract'.[164] This position betrays the influence of the 'objective theory' at the heart of traditional contract philosophy.

The particular circumstances of a purported clickwrap contract are, however, highly relevant. Notwithstanding that terms are 'signed' electronically, in accordance with traditional principle, the offeree must at least have had an opportunity to be fully informed as to the terms of the offer before communicating acceptance.[165] (It must also be made clear to the user that the act said to constitute acceptance does, in fact, have the effect of accepting contractual terms[166]). Therefore, any terms that are not made available (perhaps by way of text in a scroll box,[167] or a functional hyperlink[168]) at or prior to the moment of 'signing' will not be incorporated into the contract.[169] This will include, for example, any privacy terms purportedly incorporated by reference into website terms and conditions – but which are not made available prior to the time of acceptance.

As distinct from clickwrap contracts, browsewrap contracts raise 'serious concerns' as to their enforceability.[170] One concern is as to timing, as the terms of the contract must be sufficiently brought to the notice of the offeree *before* the contract is formed.[171] This is problematic, as the act

[162] Clapperton and Corones, see note 110, p157.
[163] Blount, see note 113, p97.
[164] Blount, see note 113, p97.
[165] Hughes and Oi, see note 112.
[166] '[A] consumer's clicking on a download button does not communicate assent to contractual terms if the offer did not make clear to the consumer that clicking on the download button would signify assent to those terms': *Specht v Netscape Communications Corp*, 306 F 3d 17 (2nd Cir, 2002), 29-30 ('*Specht*')
[167] As in the Canadian case of *Rudder v Microsoft Corp* 1999 CanLII 14923 (ON SC), in which Winkler J drew an analogy (at [14]) between terms presented in a scroll box and those in a 'multi-page written document which requires a party to turn the pages'. (See *Specht*)
[168] '[A]n electronic signature is capable of incorporating all the terms of an electronic contract where the electronic offer brings the terms of the offer to the notice of the offeree. Actual notice is given by reasonably sized text in a scroll box, even if only a portion of the text is immediately visible. A hyperlink that is functional and clearly visible may also be sufficient to put an offeree on inquiry of terms': Blount, see note 113.
[169] For example, in *eBay International AG v Creative Festival Entertainment Pty Ltd* (2006) 170 FCR 450
[170] Certainly in Australia but, Clapperton and Corones suggest, even in the United States: see note 110, p157.
[171] Blount, see note 113, p112.

often said to constitute acceptance of a browsewrap contract is use of the website, but the website must be used in order to see the purported contractual terms.[172]

Further, it is unclear whether sufficient notice will have been given to bind a user to terms of a browsewrap contract.[173] The display of terms in reasonably sized font, in a text scroll box, is likely to provide sufficient notice,[174] although this has not been established in Australia. A mere reference to the existence of terms elsewhere on the site, with a request to read them, may not, on the basis of US case law, provide adequate notice.[175]

It may be that website operators purposely do not draw users' attention to website terms (including privacy terms), given their sometimes onerous nature.[176] However, the more onerous a term, the more notice is, in fact, required in order that reliance can later be placed on it.[177]

Unusual or onerous terms (such as exclusion of liability and forum selection provisions, which are frequent in website terms) may be capable of being incorporated into an online contract through the use of clear language that draws these terms to the specific attention of the user.[178] Canadian case law suggests that a functional hyperlink to terms (which may contain onerous provisions) may also be sufficient.[179]

8.8.4. Vitiating factors

Unconscionable conduct (statutory and within meaning of unwritten law)

Sections 20 and 21 of the ACL prohibit unconscionable conduct, respectively, within the meaning of the 'unwritten law', and in 'trade or commerce' in connection with the supply or acquisition of goods or services. In section 20, the reference to 'unwritten law' is a reference to the general law.[180]

Under general law, and under section 20 of the ACL (which refers to it), a necessary element of unconscionable conduct is that the stronger party had actual or constructive knowledge of a special disability suffered by the weaker party.[181]

---

[172] As also highlighted by Clapperton and Corones, see note 113, p157.
[173] Clapperton and Corones, see note 110, p157.
[174] Blount, see note 113, p112.
[175] *Specht* – see Blount, see note 113, p103; Hughes and Oi, see note 112.
[176] Clapperton and Corones, see note 110, p157.
[177] Khoury and Yamouni, see note 122, p177. As authority for this proposition, see *Thornton v Shoe Land Parking Ltd* [1971] 2 QB 163.
[178] Blount, see note 113, p112.
[179] Blount, see note 113, p112.
[180] R Miller, *Miller's Australian Competition and Consumer Law Annotated* (Thomson Reuters (Professional), 37th ed, 2015), p 1615.
[181] Khoury and Yamouni, see note 122, p351; Halsbury's Laws of Australia (at 28 April 2015) 110 Contract, '4 Vitiating Factors' [110-5920].

Under each of the general laws, section 20, and section 21, it is also generally understood that something more than 'substantive' unconscionability is required. Therefore, the weaker party cannot rely merely on objectionable terms in a contract concluded with the stronger party. There must also have been some conduct in the process of negotiating or concluding the contract – some 'procedural' conduct – that may be considered unconscionable.

Courts in the United States have shown a willingness to intervene in contracts where 'the contract [or a term of the contract] is harsh, exorbitant or unconscionable'.[182] Whilst US courts demand evidence of both procedural and substantive unconscionability, they apply a 'sliding scale' test that requires procedural unconscionability to a lesser degree in the presence of clear substantive unconscionability.[183]

US case law provides examples of contracts or terms found to be procedurally unconscionable because users had little realistic market choice between providers,[184] or due to the existence of unequal bargaining positions and the creation of 'surprise' through hidden terms.[185] Contracts and terms have been found to be substantively unconscionable because they provided the stronger party with the ability to act unilaterally to the weaker party's detriment (for example, by unilaterally modifying contractual terms without notice).[186]

Accordingly, a 'broader approach [to the unconscionability question] is taken in the United States',[187] and Australian courts may not be greatly assisted by US precedent,[188] although an Australian court may perhaps be persuaded to find procedural unconscionability where 'a weaker party enters into a standard form contract on-line [sic] because of a lack of reasonable on-line [sic] alternatives'.[189]

It is probably unlikely that the common law, or section 20 of the ACL, would assist an individual asserting unconscionable conduct in connection with the making of, for example, a clickwrap or browsewrap contract. This is partly because of the requirement that the other party (for example, the website operator) knew, or ought to have known, of any special disability under which the weaker party was operating.[190]

---

[182] Blount, see note 113, p118.

[183] Blount, see note 113, p119.

[184] See, eg., *Comb v Paypal Inc*, 218 F Supp 2d 1165 (ND Cal, 2002):
'Californian courts have held electronic standard form contracts to be procedurally unconscionable where there have been no realistic market alternatives available to the consumer. But this position has not been adopted by all states, most importantly New York': Blount, see note 113,133.

[185] S Gindin, 'Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears' (2009) 8 *Northwestern Journal of Technology and Intellectual Property,* p16

[186] See, e.g., *Comb v Paypal*. See also Blount, see note 113, p119; Gindin, see note 185, pp16-17.

[187] Blount, see note 113, p118.

[188] Blount, see note 113, p133.

[189] Blount, see note 113, p133. This argument was made in the context of the old *Trade Practices Act 1974*, however, the provisions of the ACL do not alter it in any material respect.

[190] Blount, see note 113; see also note 93, p160.

However, it is possible that section 21 of the ACL might assist.[191] As a general proposition, this provision also requires procedural unconscionability, although there is some case law suggesting that there may be unconscionable conduct in circumstances of, for example, a 'written contract which contains "fine print" in conflict with the purported effect of the contract'.[192]

Certainly, various commentators countenance the possibility that 'one-sided terms' in online contracts – perhaps in the presence of other factors, such as a general lack of transparency resulting from legalese – may constitute unconscionable conduct.[193] Mathews-Hunt suggests (in relation to cloud computing contracts, but the argument can equally be applied to other online contracts) that 'clauses exploiting obvious inequality of bargaining power, unilateral cloud provider contract variation rights, non-negotiability, terms not reasonably necessary to protect the provider's legitimate interests – and the like – might be pleaded together in order to establish that a cloud provider has acted unconscionably towards a consumer'.[194]

Outside of contractual terms, practices which impose time limits on the period that a website user has to review and agree to terms (including privacy terms) may also be unconscionable, considering the usual length of documents containing such terms.[195]

[191] Blount, see note 113, p134.

[192] Clapperton and Corones, see note 110, p162.

[193] Hughes and Oi, see note 112. See also Mathews-Hunt, see note 131, p461.

[194] Mathews-Hunt, see note 131, p465.

[195] Clapperton and Corones, see note 110, pp174-5.

Unfair terms and unjust contracts

As the unfair contract terms provision in section 23 of the ACL is directed at the substantive content of a contract (and does not require a procedural element, as is arguably the case even in respect of section 21 unconscionability), it may be of greater assistance to an individual user who has concluded an online contract with an organisation.

In order for section 23 to apply, there must be a 'consumer contract' (for a 'supply of goods or services') that is a 'standard form contract'. Due to the broad definitions of 'goods' and 'services' in the ACL, it is likely that many contracts will fall within the meaning of 'consumer contract'. In addition, most clickwrap and browsewrap contracts will be 'standard form contracts' (if not due to the statutory presumption in section 27(1), then on the factors to be considered under section 27(2) of the ACL).

However, in order for section 23 to apply, there must nonetheless be *a* contract.[196] Due to potential deficiencies in the formation of, and incorporation of terms in, clickwrap and browsewrap contracts (as discussed above), in practice there may not be a contract to which section 23 can apply.

In this respect, it is interesting to note the case of *In re Google, Inc.*,[197] the German Federation of Consumer Associations argued the applicability of Germany's unfair contract terms legislation to Google's terms of use and privacy policy. Google responded that neither the terms, nor the privacy policy, were valid contracts as there was no exchange for value. Therefore, it was said, there was no contract to which the unfair contract terms legislation could apply.

However, the Berlin District Court rejected Google's argument, holding that there was a relevant contract based on the commercial value of the personal data collected by Google. The court then held that, under the unfair contract terms legislation, all of the 25 provisions in Google's online terms of use and privacy policy were unenforceable.

The German Google case could be persuasive in Australia.[198] Using the Google case as a guide, the types of terms that might be judged unfair under Australian legislation include: terms that allow for unilateral termination (or termination on unequal terms[199]); terms that allow for unilateral alteration of service; terms that allow unilateral variation of terms;[200] and exclusion of liability clauses.[201]

---

[196] Ashurst, 'Is your privacy policy unfair? Application of the Australian Consumer Law to privacy policies' (2015).

[197] See Mathews-Hunt, see note 131, p466.

[198] See Mathews-Hunt, see note 131, p466.

[199] By consent, the Federal Court of Australia declared a term of this type to be unfair in *ACCC v Bytecard* (Federal Court, 24 July 2013, VID301/2013).

[200] In *Director of Consumer Affairs Victoria v AAPT* [2006], the Victorian Civil and Administrative Appeals Tribunal held a term of this type to be unfair under the Victorian *Fair Trading Act 1999*, which contained unfair contract terms provisions very similar to those in the ACL: Clapperton and Corones, see note 110, p167.

[201] Mathews-Hunt, see note 131, p466. See also Ashurst, see note 196

Other types of terms that may well fall foul of the unfair terms regime include: terms allowing the giving of notice in ways which are unlikely to come to the attention of the user;[202] some choice of law and forum clauses;[203] and some mandatory arbitration clauses.[204] Where website terms are too long, and are not written in plain English, this will likely be a factor.[205]

Section 23 of the ACL may well apply to privacy policies, if they are incorporated into a standard form 'consumer contract'.[206] It is often the case that privacy policies are incorporated into broader online agreements dealing with the supply of goods or services, as in some of the examples provided in Appendix A.

Beyond the types of general contractual terms that may be judged 'unfair', potentially unfair terms that specifically appear in privacy policies include:

- Terms that attempt to obtain informed consent to overseas disclosure for the purposes of APP 8
- Terms providing for extensive collection and usage rights, including the disclosure of personal information to multiple, often unidentified, third parties
- Terms that state that the service provider is not responsible for the privacy practices of third parties (see also 6.2.7 Treatment of third party issues)
- Terms providing that the consumer is liable for, and indemnifies the service provider in respect of, any loss arising in respect of third party personal information that the individual supplies to the service provider.[207]

The effect of a finding that a contract term is 'unfair' is that that term is void.[208]

The New South Wales *Contracts Review Act 1980* may also provide assistance to consumers, although this imports obvious limitations of jurisdiction. In addition, courts applying this Act still appear to require proof of procedural unconscionability, as well as substantively unjust contractual terms.[209]

Misleading and deceptive misrepresentations

The Australian case of *eBay International AG v Creative Festival Entertainment Pty Limited*[210] shows that a party may be judged to have engaged in misleading or deceptive conduct, under the ACL, for

[202] Clapperton and Corones, see note 110, p169.
[203] Clapperton and Corones, see note 110, p172.
[204] Clapperton and Corones, see note 110, p173.
[205] Mathews-Hunt, see note 131, p462.
[206] Ashurst report, see note 196.
[207] Ashurst report, see note 196.
[208] ACL s 23.
[209] Clapperton and Corones, see note 110, p164.
[210] (2006) 170 FCR 450.

purporting to rely on terms that were not adequately brought to consumers' attention (and, therefore, were not contractually enforceable).

This case law accords with findings by US courts, under unfair trade laws similar to section 18 of the ACL, that organisations have engaged in prohibited conduct by (for example):

- not adequately disclosing, in a licence agreement and privacy statement, facts that would be material to a consumer's decision to download software;[211]and
- not complying with their privacy policies (including because they failed to keep personal information secure).[212]

In 2002, the Australian Competition and Consumer Commission (ACCC), and the then Office of the Federal Privacy Commissioner (now the Office of the Australian Information Commissioner), announced their joint intention to cooperate on privacy compliance.[213] The significance of this approach was thought to be that a company would run the risk of engaging in misleading and deceptive conduct, under the then *Trade Practices Act 1974* (now ACL), if it '[made] a statement about the way it [would] handle information in a document which is available to the public, and its practices are inconsistent with that statement'.[214]

In 2012, there was renewed thought by practitioners that this approach, prompted by successful cases in the US, might be adopted, with the ACCC and/or individuals (or competitors) taking action under section 18 of the ACL for non-compliance with privacy policies.

Accordingly, non-compliance with the terms of a privacy policy, or website terms of use, may result in a successful action for misleading and deceptive conduct (as well as an action for breach of contract, if the term is a contractual one). Equally, 'burying important terms in fine print' may constitute misleading and deceptive conduct under the ACL.[215]

As 'puffery' may in some circumstances be conduct falling under section 18, it should be queried whether ubiquitous statements such as 'We take your privacy seriously' and 'We do everything possible to protect your personal information' (when neither is a reflection of reality) might in certain circumstances be misleading or deceptive. See also 6.3.1 Meeting communications challenges.

It will not be material that the relevant conduct occurs overseas, as long as the conduct (for example, a statement) is directed to Australia.[216]

8.9. Conclusion

[211] *Sears Holding Management Corp*, FTC Matter No 0823099, Docket No C-4264 – in Gindin, see note 185,
[212] DLA Piper, 'Developing US privacy trend that will soon impact Australian businesses'.
[213] Lyne, 'Regulators team up on privacy compliance', p353.
[214] Lyne, 'Regulators team up on privacy compliance', p354.
[215] Blount, see note 113, p45. See also Clapperton and Corones, see note 110, p163.
[216] Blount, see note 113, p146.

The features of the contracting model proposed by traditional contract theory – such as individual autonomy, legal capacity, freedom of choice, and perfect understanding – are not necessarily present when parties purport to conclude standard form browsewrap contracts. As seen in Appendix A, many online privacy policies are, or form part of, standard form browsewrap contracts.

Standard form contracts, and particularly standard form browsewrap contracts, challenge the traditional contracting model and raise a number of issues concerning enforceability and fairness. For example, it is possible that transacting individuals lack legal capacity to contract, and are not notified of terms in a manner sufficient for these to properly form part of any concluded agreement.

Further, standard form browsewrap contracts (and privacy terms within them) risk breaching legislative provisions on unconscionable conduct, unfair terms, and misleading and deceptive conduct. Apart from the possible legal ramifications of many browsewrap contracts, reliance upon these as a means by which to bind consumers risks undermining the confidence and trust of the consumer. A better practice on the part of service providers, which is more in line with traditional notions of contract and that has the consumer's interests at heart, would be for service providers to take a more active approach in alerting consumers with respect to contracts – both the fact that they exist and the important terms and conditions that contracts purport to make binding.

The need for an objective test of contract will always be present as a practical means by which to indicate the existence of a contract – however, a stricter insistence on the philosophical basis of the traditional contracting model, based on consumer autonomy, capacity, freedom and understanding, would address some current deficiencies in the way in which consumers provide consent for privacy purposes.

Key issues

1. The legal validity of clickwrap and browsewrap contracts – have contracts been formed with consumers?
2. Should privacy concerns be the subject of these types of contracts?
3. Whether privacy policies should be contractual – are contracts required by service providers in order to collect and use personal information in the ways described in privacy policies?
4. The terms in consumer contracts and privacy policies that may be considered 'unfair'? For example:
    - Terms that attempt to obtain informed consent to overseas disclosure for the purposes of APP 8
    - Terms providing for extensive collection and usage rights, including the disclosure of personal information to multiple, often unidentified, third parties
    - Terms that state that the service provider is not responsible for the privacy practices of third parties
5. Terms providing that the consumer is liable for, and indemnifies the service provider in respect of, any loss arising in respect of third party personal information that the individual supplies to the APP entity
6. Possible aspects of unconscionable conduct when considering privacy policies as a whole:
    - Clauses exploiting obvious inequality of bargaining power
    - Unilateral right to vary contract
    - Non-negotiability

Appendix A – Privacy policy comparative analysis table[217]

Mobile app publishers – Presentation of privacy information

Entity	Accessibility and length	Contractual issues	Self-regulatory scheme - other	Security claims
Super-cell	• 3440 words • Via app store page (eg. Appendix B, Image 3)	• Agree to contract through use of service. • Agree to privacy policy through use of service • Informs you how you can opt out.	TRUSTe	'Supercell takes reasonable measures to protect your information from unauthorised access or against loss, misuse or alteration by third parties.' *No data breach notification policy*
Glu	• 1898 words • Via app store page (eg. Appendix B, Image 3)	• Agree to contract through use of service. • Agree to privacy policy through contract	No statement on this found.	'Glu takes reasonable measures to help protect information about you from loss, theft, misuse and unauthorised access, disclosure, alteration or destruction.
Kabam	• 7779 words • Via app store page (eg. Appendix B, Image 3)	• Agree to contract through use of service. • Agree to privacy policy by using service	TRUSTe EU-US Safe Harbor framework	'Kabam takes commercially reasonable security measures to protect against unauthorised access to, or unauthorised alteration, disclosure or destruction of, sensitive data that you share and we collect and store.' Uses SSL to protect sensitive personal information.

[217]The privacy policies in this analysis were sourced online and were current as of 20 August 2015.

Entity	Accessibility and length	Contractual issues	Self-regulatory scheme - other	Security claims
Tencent	• 3442 words • Via app store page, (eg. Appendix B, Image 3)	Agree to contract through use of service.	No statement on this found.	'We use a variety of security technologies and procedures for the purpose of preventing loss, misuse, unauthorised access or disclosure of information.' Uses SSL to protect sensitive personal information

Mobile app publishers – Collection of personal information

Entity	What information is collected?	Treatment of third party issues	Data retention	Overseas transfers
Super-cell	• User supplied data (surveys, competitions etc.) • Device data • Use information • Cookie tracking data • Social media sign-in (name, email, age etc.); social media posts and messages • 3rd party collection for behavioural advertising	Takes no responsibility for third party collection of personal information. User must read third party privacy policy (no links provided).	No clear end of data retention period	Yes. User 'consents' to overseas transfer.
Glu	• User supplied data (surveys, competitions etc.) • Device data • Use information • Cookie tracking data • Social media sign-in (name, email, age etc.); social media posts and messages • 3rd party collection for behavioural advertising	No responsibility for third party use of personal information.	No statement on this found.	No statement on this found.
Kabam	• User supplied data (surveys, competitions etc.) • Device data • Use information • Cookie tracking data • Social media sign-in (name, email, age etc.); social media posts and messages • 3rd party collection for behavioural advertising • Friend referrals	Third party use of personal information is subject to third party's privacy policy (no links provided).	No clear end of data retention period – data may persist after account is deleted (it may exist in social media and with third parties)	Data will be stored on servers in the US.

Entity	What information is collected?	Treatment of third party issues	Data retention	Overseas transfers
Ten-cent	• User supplied data (surveys, competitions etc.) • Device data • Use information • Cookie tracking data • Social media sign-in (name, email, age etc.); social media posts and messages • 3rd party collection for behavioural advertising	'…we will use reasonable efforts to ensure that such third parties only use your Personal Information: 1. In compliance with this privacy policy, 2. Subject to any other instructions we give them…'	No clear end of data retention period.	'We operate and may continue to operate servers in a number of jurisdictions around the world, so the server on which your Personal information is used may not be in your jurisdiction.'

Web browsers – Presentation of privacy information

Service provider	Accessibility and length	Contractual issues	Self-regulatory scheme - other	Security claims
Firefox (Mozilla policy)	• 995 words • Via link on download page	• No attempt to bind users to privacy policy. • Browser use subject to Mozilla public licence	No statement on this found.	'We implement physical, business and technical security measures. Despite our efforts, if we learn of a security breach, we'll notify you so that you can take appropriate action.'
Safari (Apple policy)	• 3157 words • Via link on download page	• Agreement by clicking 'agree'. • Licence agreement with user incorporates privacy policy.	TRUSTe	Separate security guidelines.
Opera	• 3002 words • Via link on download page	• Terms of service states that the user agrees to terms of service and privacy policy by using the service. • Privacy policy makes no statement that the user is bound • Onus on user to check privacy policy for updates	No statement on this found.	'Opera Software strictly protects the security of personal information within the confines of Opera's products and services and honours the users' choices for its intended use. We have safeguards in place to protect users' data from loss, misuse, unauthorised access, alteration, or destruction. We protect user data from disclosure, with exceptions only in matters where designate by law or court order.'
Internet explorer	• 7396 words • Via link on download page. • Note – much of the statement is dedicated to how to change settings.	• Users agree to terms of use by using services. • Not clear that user 'accepts' privacy policy through use. • Occasionally update privacy statement – no notification, user must check policy.	No statement on this found.	'Microsoft is committed to protecting the security of your information. We use a variety of security technologies and procedures to help protect your information from unauthorised access, use or disclosure. For example, we store the personal information you provide on PC systems with limited access, which are located in controlled facilities'.

Web browsers – Collection of personal information

Service provider	What information is collected?	Treatment of third party issues	Data retention	Overseas transfers
Firefox (Mozilla policy)	• Device data • Directly provided data (eg crash reports) • For product updates • From other sources (eg email providers) • No data collected for direct marketing • Separate cookies policy • *Possible false distinction between 'personal information' and 'non-identifiable information'.*	3rd parties contractually obligated to handle data in ways approved by Mozilla.	'We also don't want your personal information for any longer than we need it, so we only keep it long enough to do what we collected it for. Once we don't need it, we take steps to destroy it unless we are required by law to keep it longer.'	No statement on this found.
OS Safari (Apple policy)	• Broad personal information collection policy • Difficult to distinguish collection practices for specific browser • *Possible false distinction between 'personal information' and 'non-identifiable information'.*	'Information collected by third parties, which may include such things as location data or contact details, is governed by their privacy practices. We encourage you to learn about the privacy practices of those third parties.'	No statement on this found.	'All information you provide may be transferred or accessed by entities around the world as described in this privacy policy'.
Opera	• Data collected for product improvements • Data collected for marketing purposes • Search data is sent to third-parties for processing • *Possible false distinction between 'personal information' and 'non-identifiable information'.*	'Opera Software does not control the privacy and security practices and policies of… third parties and their sites.'	No statement on this found.	No statement on this found.

Service provider	What information is collected?	Treatment of third party issues	Data retention	Overseas transfers
Internet Explorer	'The information we collect from you will be used by Microsoft and its controlled subsidiaries and affiliates to turn on the features you're using and provide the services or carry out the transactions you've requested or authorised.' *No other information about types of information collected*	Information is not transferred to third parties without consent of the user.	No statement on this found.	No statement on this found.

Search engines – Presentation of privacy information

Service provider	Accessibility and length	Contractual issues	Self-regulatory scheme - other	Security claims
Google	• 2760 words • Additional document on advertising and cookie use	• Use of site binds user to terms of service and terms of privacy policy. • May update privacy policy from time to time (Thirteen times since start of 2010)	No statement on this found.	• 'We encrypt many of our services using SSL • We review our information collection, storage and processing practices, including physical security measures, to guard against unauthorised access to systems.'
Yahoo! (note: Yahoo!7 has its own privacy policy)	• 1408 words + 430 words on Yahoo Search + 834 words in topics.	• Use of site binds user to terms of service and privacy policy. • Yahoo may update policies.	Participates in US-EU safe harbour scheme.	• 'We limit access to personal information about you to employees who we believe reasonably need to come into contact with that information to provide products or services to you or in order to do their jobs. • We have physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you.'
ChaCha	2428 words	Use of site binds user to terms of use and privacy policy	No information provided.	'To improve data security and restrict access to your personal and business information, ChaCha has put in place certain physical, electronic, and managerial procedures to safeguard the information ChaCha collects via the Site.'

Service provider	Accessibility and length	Contractual issues	Self-regulatory scheme - other	Security claims
DuckDuck Go	2139 words	• No terms of use. • Privacy policy is not a contract.	No statement on this found.	Site does not collect personally identifiable information.

Search engines – Collection of personal information

Service provider	What information is collected?	Treatment of third party issues	Data retention	Overseas transfers
Google	• Information provided by users • Device information • Use information • Search queries • Info from other Google services to provide users with 'tailored content'. • 'Share' non-personally identifiable information publicly and with partners. • DoubleClick cookie information is not combined with other information.	Third parties who serve behavioural ads are not covered by Google's privacy policy.	No statement on this found.	No statement on this found.
Yahoo!	• Device information • Registration data provided by users with regard to competitions etc. • For 3rd party advertising • Pages that users request.	No statement on this found.	No statement on this found.	No statement on this found.
ChaCha	• 'ChaCha may request and/or collect personal information from you that may include: first and last name, address, phone number, email address, location or other information.' • Automatically records all search queries or questions. • Use data. • 3rd party advertisers, serving ads based on tracking data.	No statement on this found.	'If you ever wish to access your personal information, or to have your personal information deleted, updated, changed or modified, you may contact ChaCha…"	ChaCha processes and stores information in the USA.
DuckDuckGo	• Searches are saved but not in a personally identifiable way. • No cookies are used by default.	Third parties do not receive personal information.	No personal information is collected.	No personal information is collected.

Social media – Presentation of privacy information

Service provider	Accessibility/ presentation issues/ length	Contractual issues	Self-regulatory scheme/ other	Security claims
Facebook	• 2,700 words • Via link on Facebook home page	• Agree to contract through use of service • Agree to privacy policy through contract • Facebook may vary contract and privacy policy – users bound by changes by continued use.	TRUSTe US-EU and US-Swiss Safe Harbor	'We work hard to protect your account using teams of engineers, automated systems, and advanced technology such as encryption and machine learning. We also offer easy-to-use security tools that add an extra layer of security to your account'.
Instagram	• 2,791 words • Via link on Instagram home page	• Agree to contract through use of service • Agree to privacy policy through use of service • Instagram may vary contract and privacy policy – users bound by changes by continued use.	No statement on this found.	No specified security measures. Instagram uses 'commercially reasonable safeguards' to keep information secure.
Twitter	• 3,189 words • Via link on Twitter home page	• Agree to contract through use of service • Agree to the terms of privacy policy through contract, which is agreed to through use of service • Twitter may vary contract and privacy policy. Users bound by changes by continued use.	US-EU and US-Swiss Safe Harbor	No specified security measures.

Service provider	Accessibility/ presentation issues/ length	Contractual issues	Self-regulatory scheme/ other	Security claims
Snapchat	• 3,080 words • Via link on Snapchat home page	• Agree to contract through use of service • Agree to privacy policy through contract • Snapchat may vary contract and privacy policy -- users bound to changes by continued use.	No statement on this found.	No specified security measures.

Social media – Collection of personal information

Service provider	What information is collected?	Treatment of third party issues	Data retention	Overseas transfers
Facebook	• User supplied data (including posts and messages) • Device data • Use information • Cookie tracking data (see Cookies Policy) • Information from third party websites, apps etc.	'Non-personally identifiable information' shared on basis that advertiser agrees to Facebook advertiser guidelines.	Information retained for 'as long as it is necessary to provide products and services to [the user] and others'.	Yes. Users (and non-users) 'consent' to transfer to the US
Instagram	• User supplied data • Device data • Use information • Cookie tracking data • Contacts information through 'Find friends' feature • 3rd party collection of personal data for behavioural advertising	• Information provided to third party advertising partners: no obligations specified. • No obligations regarding anonymised and de-identified aggregated data.	When user terminates or deactivates account, Instagram (and others) may retain information 'for a commercially reasonable time for backup, archival and/or audit purposes'.	Yes. Users 'consent' to transfer to the US and any other countries in which Instagram or members of the Instagram group maintain facilities
Twitter	• User supplied data (including content metadata) • Device data • Use information • Cookie tracking data (in accordance with 'Twitter's use of cookies and similar technologies' page) • 3rd party collection of personal data for behavioural advertising	Information provided to service providers shared subject to obligations 'consistent with' the privacy policy and 'any other appropriate confidentiality and security measures'.	Log data deleted or de-identified after a maximum of 18 months.	Yes. Users 'consent' to transfer to the US, Ireland, and 'other countries'

Service provider	What information is collected?	Treatment of third party issues	Data retention	Overseas transfers
Snapchat	• User supplied data (including message content) • Device data • Use information • Cookie tracking data • Device content metadata (with consent) • Contacts information • 3rd party collection of personal data for behavioural advertising	Information provided to service providers: no obligations specified. No responsibility for third party collection or use of information.	Generally, no guarantee that messages will be deleted within a specific timeframe Messages deleted automatically from servers once viewed by recipient (*this claim has been challenged - see note 73*)	Yes. Users 'consent' to transfer to, and processing in, the US and 'other countries'

Appendix B - Accessibility of Privacy Information

Image 1: Google home page, showing links to privacy policy and terms of service

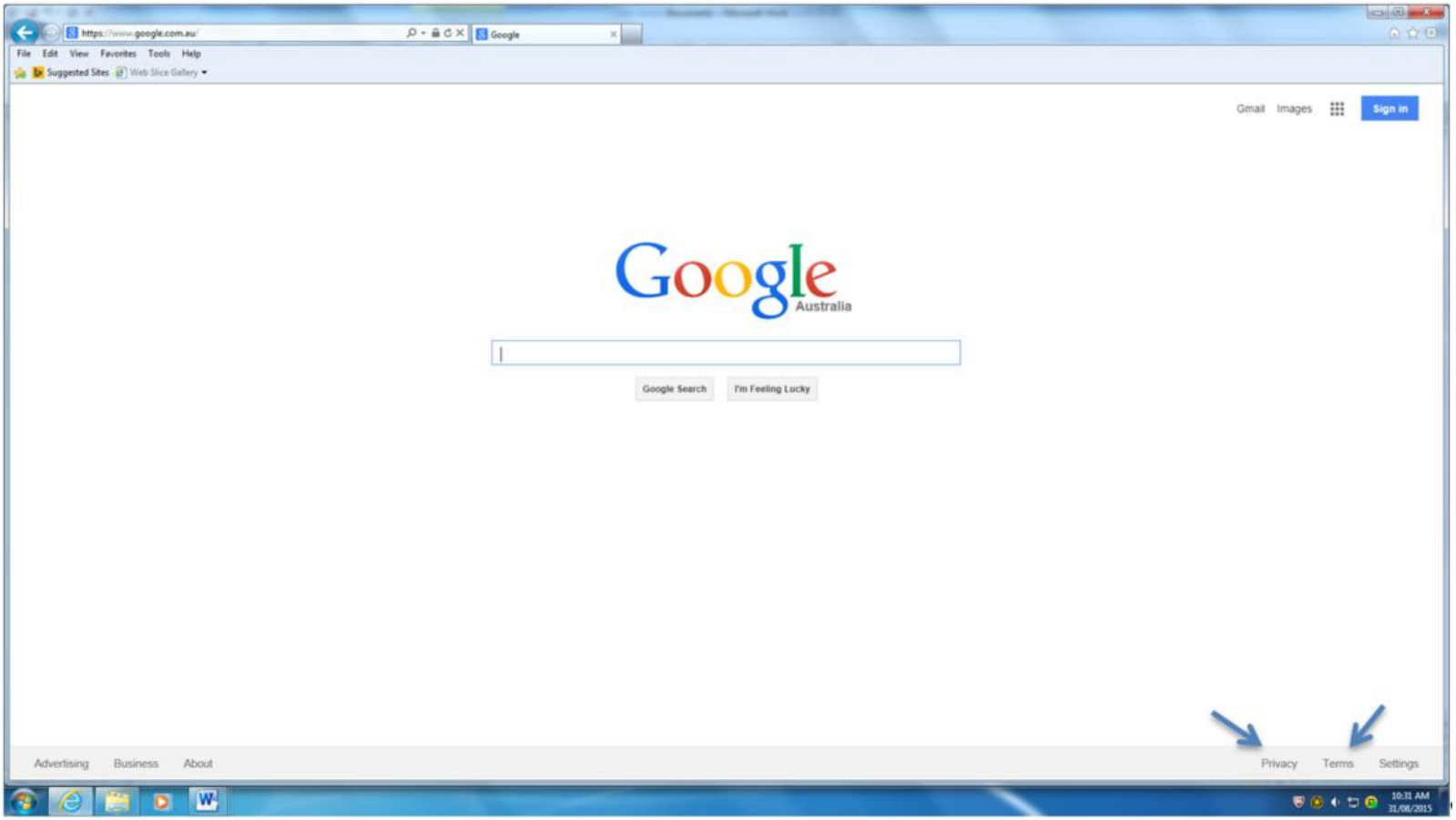


Image 2: Google home page, showing links to privacy policy and terms homepage

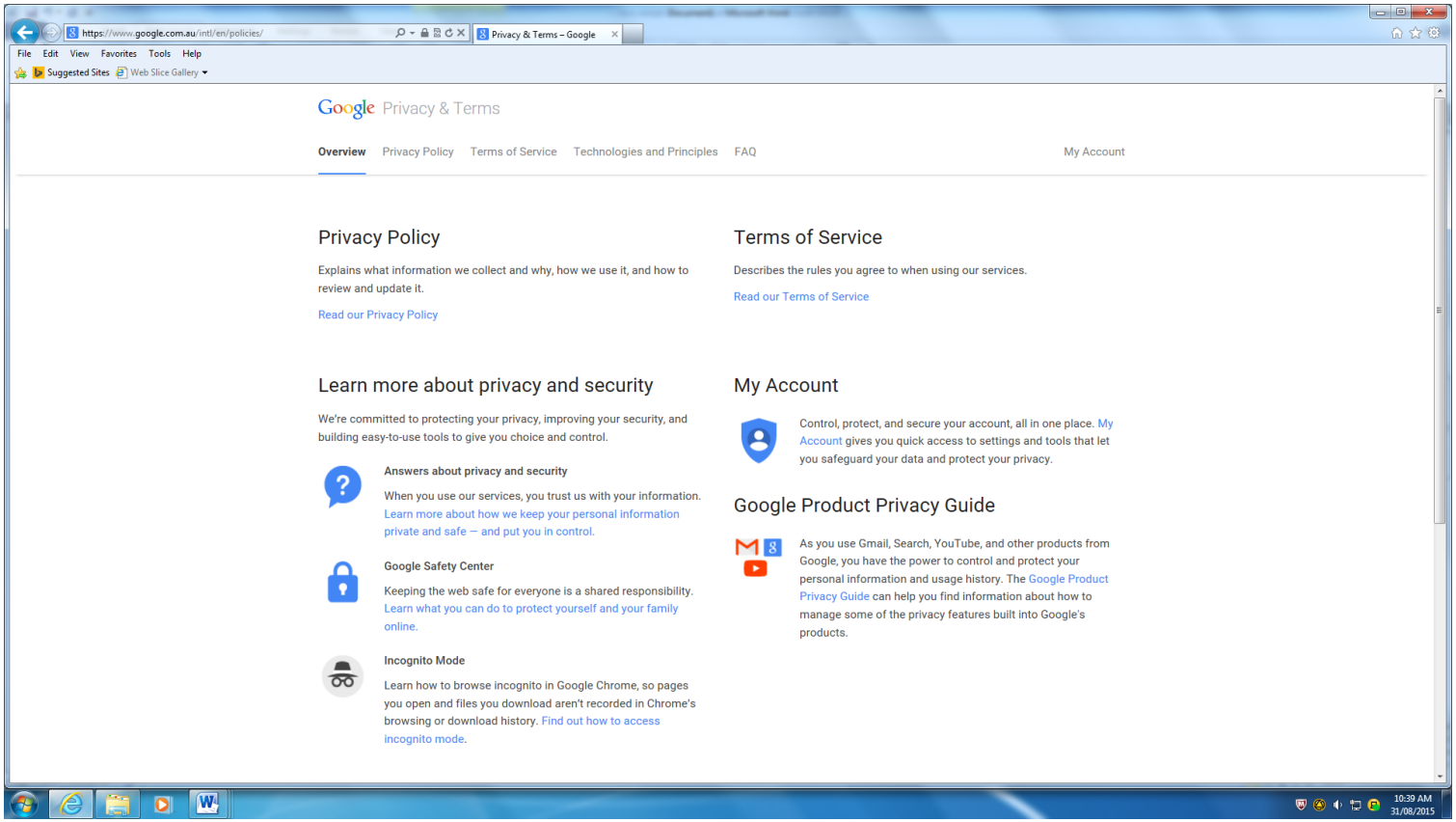


Image 3: Kabam search in app store

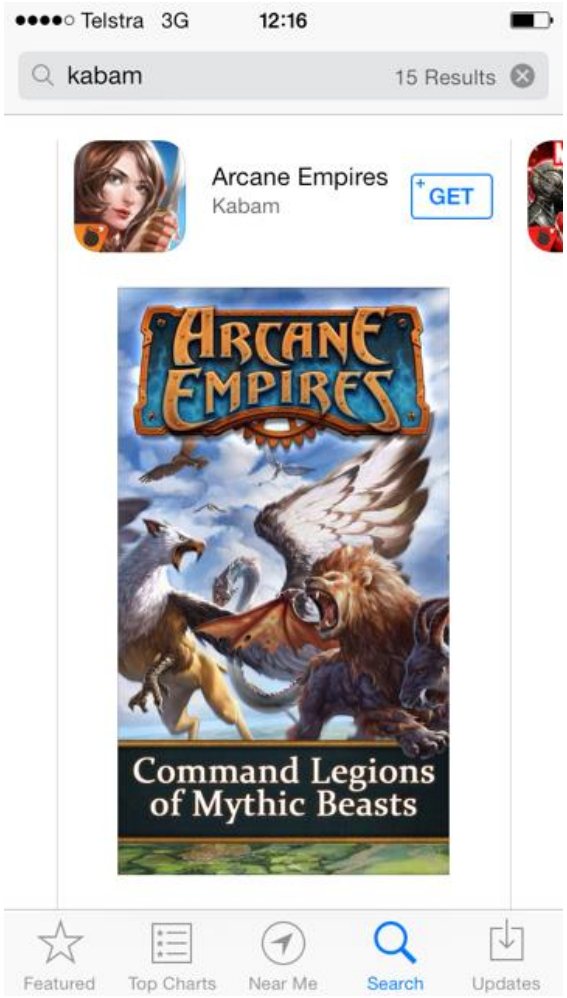


Image 4: Kabam description page

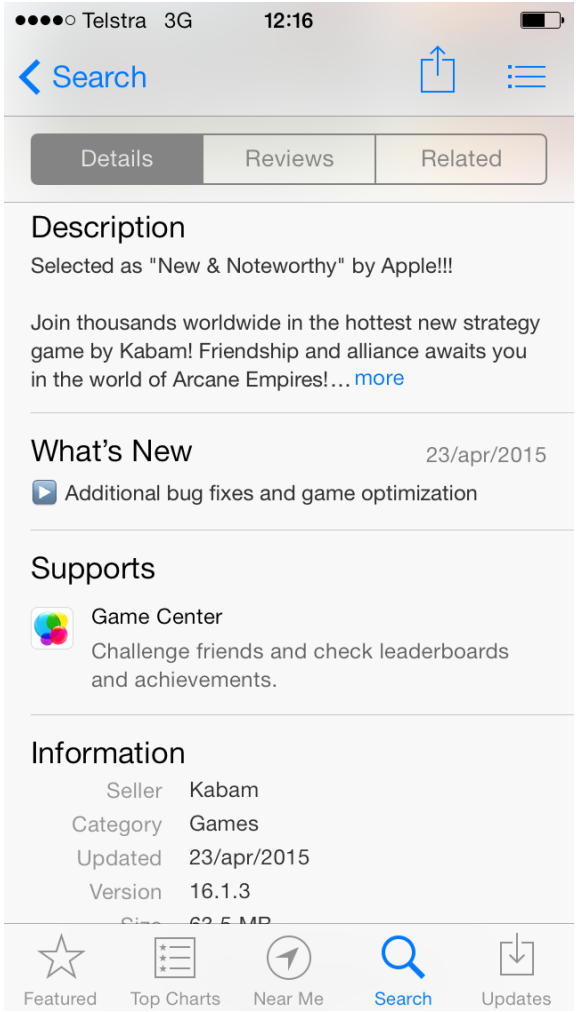


Image 5: Kabam description page continued

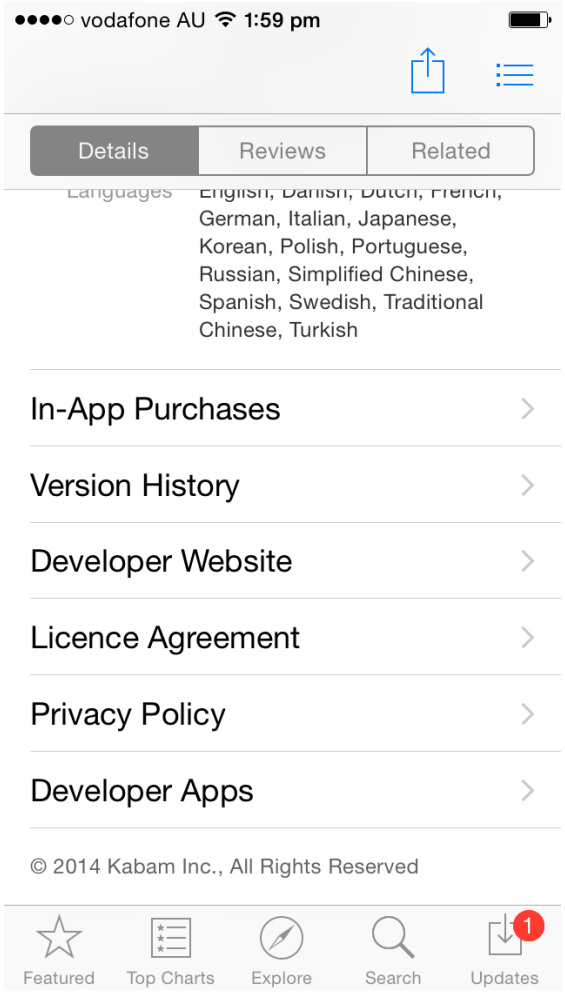
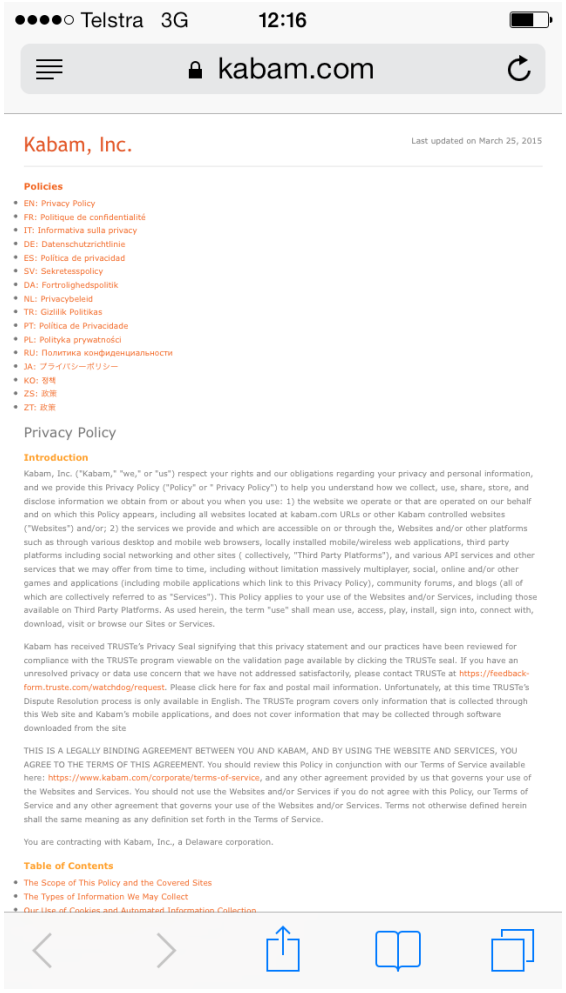


Image 6: Kabam privacy policy



Appendix C – Basic concepts in contract law[218]

1. Offer and acceptance

Offer (by the 'offeror') and acceptance (by the 'offeree') are, generally, essential elements of the agreement that creates a legally enforceable contract. Where a 'manifestation of mutual assent [can] be implied from the circumstances', courts may be willing to find the existence of a contract, even in the absence of identifiable offer and acceptance.

Acceptance must be absolute and unqualified, and must be of the exact terms offered by the offeror. If the offeree purports to introduce new terms of a material nature, this is likely to constitute a counter-offer.

Whilst the offeror may specify the manner in which the offer is to be accepted (including by certain conduct), silence – that is, the omission to do something – may not constitute acceptance.

The signature of the offeree has long been taken to constitute acceptance.

As a general proposition, acceptance of an offer should be notified by the offeree to the offeror. However, in some circumstances, it may not be necessary for the offeree to specifically notify acceptance to the offeror. Where the offeror makes clear, in the terms of the offer, that acceptance will be manifested by the performance of certain conditions, it will be sufficient that the offeree performs those conditions.

2. Intention to create legal relations

Along with offer and acceptance, a binding contractual agreement requires the parties to manifest an intention to create legal relations (that is, an intention to be legally bound).

Where the parties expressly state that this is their intention, the task of discerning the requisite intention is made easier.

However, it is usually necessary for courts to investigate whether an intention to create legal relations can be inferred, as a matter of fact, in the circumstances.

In commercial agreements, as distinct from domestic agreements (that is, agreements between friends or family members, and other agreements not typically on arm's length terms), there is a presumption that the parties do intend their agreement to create legal relations. That is, there is a presumption that the parties intend their agreement to be legally enforceable.

It is possible for a party to argue that this presumption should not be applied, however, this will be a difficult argument to make. It will not typically succeed unless there is clear evidence showing an intention to avoid contractual liability.

[218] Sources for this section are Khoury, Daniel and Yvonne Yamouni, *Understanding Contract Law* (2010) and Seddon, Nicholas and Manfred Ellinghaus, *Cheshire and Fifoot's Law of Contract* (2008)

3. Consideration

Generally, a legally enforceable contract also requires evidence of 'consideration'.

Consideration is constituted by a 'benefit or advantage' accruing to one contracting party, or a 'detriment … or inconvenience' suffered by the other.

Consideration can be constituted by the doing of an act, or the refraining from doing an act, in response to a promise. If the act is done before the making of the promise, and independently of it, it will be 'past' consideration and therefore not valid.

Consideration can also be constituted by a promise to do something (or refrain from doing something) in response to a promise.

There must be a connection between the consideration and the promise under the agreement, such that the consideration is the 'price' paid for the promise.

Consideration must be something of value, although it is for the parties, not the courts, to determine the adequacy of the consideration with respect to the promise.

The party receiving the benefit of a promise must show that he or she has provided consideration, if seeking to enforce that promise.

4. Legal capacity

There is a general presumption, under common law, that a person who enters into a contract has legal capacity to do so (and that the contract is, therefore, enforceable).

However, on the basis that 'certain persons may not be capable of assessing the real meaning of a contract and the obligations created by it', some categories of person are considered to not have full contracting capacity. These categories include minors, mentally disabled people, and intoxicated people.

The party alleging that the contract is not enforceable bears the onus of proving their incapacity (for example, that they were so intoxicated at the time of contracting that they did not understand what they were doing, and that the other party knew, or ought to have known, of their condition). If this party is successful, often the contract may be avoided at their option.

5. Incorporation of terms

According to a long tradition in case law, a person is bound by all express terms of a contract to which they have assented by signing the document containing those terms. This is so except in the presence of vitiating factors: fraud or misrepresentation.

Generally, it is immaterial that the person may not have read the document.

However, a more recent line of cases suggests a party may not be bound to terms excluding liability where the document signed by that party was not presented in such a way as to indicate that it contained contractual terms.

Where purported terms of a special, onerous or unreasonable nature are contained in an *unsigned* document, a court must instead consider:

- whether a reasonable person would consider the document to be contractual in nature; and
- if so, whether reasonable notice of the purported terms was given.

If the document is one that a reasonable person would consider contractual in nature, the question becomes whether reasonable notice was given of the terms upon which reliance is placed. 'Standard form' contracts often give cause to consider this question.

Specifically, on the question of reasonable notice, courts consider the visibility, legibility, and availability of terms to the recipient. The recipient of standard form terms must have a sufficient opportunity to read the terms relied upon – and importantly, must have this opportunity *prior* to the conclusion of the contract (that is, prior to acceptance of the offer).

This is a factor when a party seeks to incorporate terms 'by reference' - that is, by making reference in a (signed or unsigned) document to unsigned terms set out elsewhere, and seeking to incorporate these in the primary document.

Courts are likely to require particularly onerous clauses – such as broad exclusion of liability clauses – to comply with a higher standard of notice. Of an exclusion clause posted in a car park, it was said that the clause was 'so wide' and 'so destructive of rights' that a person could not be bound by it unless their attention was drawn to it 'in the most explicit way' – for example, by printing it 'in red ink with a red hand pointing to it – or something equally startling'.

Along with the express terms agreed by the parties, all contracts contain implied terms, such as the 'universal' implied term requiring both parties to do all things necessary to enable the other to enjoy the benefit of the contract.

6. Vitiating factors

The presence of a vitiating factor typically has the effect of rendering the contract void or voidable. Only some vitiating factors are discussed here. Others, such as duress, are beyond the scope of this report.

6.1. Misrepresentation

Whilst there is a body of common law dealing with the matter of misrepresentation inducing entry into contracts, parties arguing misrepresentation now often rely on legislative provisions.

Accordingly, broad and flexible legislative provisions such as section 18 of the ACL have largely superseded the common law in this area.

6.2. Unconscionable dealing

In limited circumstances evidencing unconscionability, courts exercising equitable jurisdiction are willing to intervene in contractual transactions.

Courts do not have jurisdiction to intervene merely on the basis of 'unfairness' in a contract, but are willing to intervene where:

- one contracting party suffered from a 'special disability', putting them at a 'disadvantageous position' with respect to the other; and
- the other party unconscientiously took advantage of that position.

Once these two factors are proven, the onus falls to the stronger party to establish that the transaction was, in fact, fair and reasonable and not oppressive.

Mere inequality of bargaining power is unlikely to give rise to a 'special disability' in the eyes of the law. However, it is possible that lack of assistance or explanation, where assistance or explanation is necessary, will be sufficient. Likewise, infirmity, illiteracy, and inexperience or lack of education have been recognised as categories of special disability.

In order for a special disability to be exploited, there must be knowledge of the disability to some extent. It is necessary that the stronger party knew, or ought in the circumstances to have known, of the disadvantage. Further, it is necessary that the disadvantage was such that it was unconscientious for the stronger party to accept the weaker party's assent to the transaction.

Where a court finds unconscionability, the contract becomes voidable. As an alternative, the court may adjust the innocent party's liability under the contract.

Unconscionability may also constitute a breach of legislation.

6.3. Mistake

'In the absence of some other vitiating factor, … the mistaken party is usually left to suffer the consequences of their mistake'.

However, there are some limited grounds on which a court will intervene to 'correct' the effects of a mistake on the part of a contracting party. The assumption underlying such interventions is that the parties have not truly 'agreed' where the contract is affected by mistake.

The consequences of a court's intervention will depend upon the nature of the mistake ('common', 'mutual', or 'unilateral' mistake), and whether proceedings are brought in common law, or a court's 'equitable' jurisdiction (which has traditionally allowed courts greater discretion in determining outcomes).

In some circumstances – such as where the parties are found to have operated under a common mistake as to a matter fundamental to the contract – the contract will be rendered void.

Where a party is found to have operated under a 'unilateral' mistake, and the other knew, or should have known, of this, the consequences will depend to a large degree on the circumstances. The general principle is that 'a unilateral mistake will be of no consequence unless it is fundamental to the contract'.

6.4. Undue influence

Similar to the vitiating factor of duress, undue influence requires consideration of the quality of the parties' consent. Can it be said that the parties both exercised free will in making the decision to contract?

In certain categories of recognised relationship (such as doctor and patient, and solicitor and client), it is presumed that undue influence was exercised over the weaker party, unless the stronger party can rebut this presumption. The list of 'special' categories of relationship is not closed.

In other cases, whilst the relationship between the contracting parties cannot be said to fall within any 'special' relationship, the circumstances are such that there can be said to be 'actual' undue influence.

'Actual' undue influence features unfair or improper conduct by the stronger party, as proved by the weaker party. Frequently, there will be no consideration, or inadequate consideration, moving from the stronger party to the weaker party. Similarly, it may be a factor that the terms of the contract are notably favourable to the stronger party.

The remedy for undue influence is an order by the court setting aside the contract or confirming rescission.

Undue influence may also constitute a breach of legislation.

Appendix D - Legislation dealing with unconscionable conduct

i) Commonwealth legislation prohibiting unconscionable conduct in certain transactions

Section 21 of the Australian Consumer Law[219] prohibits unconscionable conduct in trade or commerce, in connection with the supply or possible supply of goods or services to a person.

Section 21 is discussed before ACL section 20 (which prohibits conduct that is unconscionable within the meaning of the 'unwritten law'), as section 20 is expressed to apply only if section 21 does not.[220]

The text of section 21 makes clear that the section is 'not limited by the unwritten law relating to unconscionable conduct'[221] (which is the province of section 20).

In applying section 21 to determine any breach by the supplier, a court may have regard to the non-exhaustive list of factors in section 22(1), including, relevantly,

- 'the relative strengths of the bargaining positions of the supplier and the customer';[222]
- 'whether the customer was able to understand any documents relating to the supply or possible supply of the goods or services';[223]
- 'the extent to which the supplier unreasonably failed to disclose to the customer:
    - any intended conduct of the supplier that might affect the interests of the customer; and
    - any risks to the customer arising from the supplier's intended conduct (being risks that the supplier should have foreseen would not be apparent to the customer)';[224] and
- 'without limiting [the foregoing paragraph], whether the supplier has a contractual right to vary unilaterally a term or condition of a contract between the supplier and the customer for the supply of the goods and services'.[225]

If the conduct relates to a contract, the court may also consider the extent which the supplier was willing to negotiate the terms and conditions of the contract with the customer.[226]

[219] *Competition and Consumer Act 2010* (Cth) sch 2 ('ACL').
[220] ACL s 20(2).
[221] ACL s 21(4).
[222] ACL s 22(1)(a).
[223] ACL s 22(1)(c).
[224] ACL s 22(1)(i).
[225] ACL s 22(1)(k).
[226] ACL s 22(1)(j).

Whilst the meaning of 'unconscionable' conduct under section 21 is expressed to be broader than the meaning of unconscionable dealing under general law,[227] there are recognised limitations in the application of the provision. For example, in order to activate the provision:

- there must generally be some relevant circumstance beyond the mere terms of the contract (that is, there must be 'procedural' unconscionability, not just 'substantive' unconscionability);[228]
- something more than inequality of bargaining power between the parties is required, as the supplier must have taken advantage of any inequality;[229] and
- something more than a lack of understanding of a supply contract, on the part of the customer, is required.[230]

ii) Commonwealth legislation prohibiting conduct which is unconscionable within the meaning of the unwritten law from time to time

Section 20 of the ACL prohibits conduct which is unconscionable within the meaning of the unwritten law from time to time.

The reference to 'unwritten law' is a reference to the general law.[231]

It is possible that section 20 has a wider scope than is provided by the classic test for unconscionability at general law.[232] Yet, as the case law currently stands, it is likely that the elements of 'traditional' unconscionability are required to make out a case under section 20.

Legislation dealing with unfair contract terms

The Victorian *Fair Trading Act 1999* introduced a regime for consideration of unfair contract terms in 2003.[233]

Since then, a national legislative regime dealing with unfair contract terms has been introduced by way of the ACL.

Section 23 of the ACL provides that a term in a standard form consumer contract is void if that term is unfair.

---

[227] ACL s 21(4).

[228] Miller, see note 180, p1624.

[229] Miller, see note 180, p1634. See also Clapperton and Corones, see note 110, on one of the predecessors to section 21 (section 51AB of the *Trade Practices Act 1974* (Cth).

[230] Miller, see note 180, p1626.

[231] Miller, see note 180, p1615.

[232] Clapperton and Corones, see note 110. See also Attorney-General's Department (Cth), *Contract law and consumer law* (24 October 2012) - http://bit.ly/1UTMKLo

[233] Miller, see note 180, p1635.

If a contract is for 'a supply of goods or services … to an individual whose acquisition of the goods, services or interest is wholly or predominantly for personal, domestic or household use or consumption', then it falls within the definition of a 'consumer contract'.[234] Both 'goods' and 'services' are defined inclusively in the ACL,[235] meaning that these terms may be interpreted broadly.

If one party alleges that the contract being considered is a standard form contract, then under the ACL there is a rebuttable presumption that this is so.[236] A court may, however, determine otherwise upon proof by the other party.[237] In making its determination, the court must take into account the factors set out in ACL section 27(2).

[234] ACL s 23(3).
[235] ACL s 3.
[236] ACL s 27(1).
[237] ACL s 27(1).

A term of a standard form consumer contract will be unfair (and therefore void) if it satisfies the three requirements under section 24(1) ACL:

- 'it would cause a significant imbalance in the parties' rights and obligations arising under the contract';[238]
- 'it is not reasonably necessary in order to protect the legitimate interest of the party who would be advantaged by the term';[239] and
- 'it would cause detriment (financial or otherwise) to a party if it were to be applied or relied on'.[240]

In making the assessment under section 24, a court must consider:

- 'the extent to which the term is transparent'[241] (expressed in reasonably plain language, legible, presented clearly, and readily available to any party affected by the term[242]); and
- 'the contract as a whole'.[243]

Section 26 of the ACL exempts certain types of terms from the application of section 23.

Section 25 of the ACL provides examples of the types of terms that may be unfair, including:

- 'a term that permits, or has the effect of permitting, one party (but not another party) to avoid or limit performance of the contract';[244]
- 'a term that permits, or has the effect of permitting, one party (but not another party) to vary the terms of the contract';[245]
- 'a term that permits, or has the effect of permitting, one party unilaterally to … interpret [the contract's] meaning';[246]
- 'a term that limits, or has the effect of limiting, one party's right to sue another party'.[247]

If a term is deemed to be unfair (and therefore void), the contract continues to bind the parties, so long as it is capable of operating without the unfair term.[248]

Legislation dealing with unjust contracts

[238] ACL s 24(1)(a).
[239] ACL s 24(1)(b).
[240] ACL s 24(1)(c).
[241] ACL s 24(2)(a).
[242] ACL s 24(3).
[243] ACL s 24(2)(b).
[244] ACL s 25(1)(a).
[245] ACL s 25(1)(d).
[246] ACL s 25(1)(h).
[247] ACL s 25(1)(k).
[248] ACL s 23(2).

The New South Wales *Contracts Review Act 1980* allows relief in respect of 'unjust' contracts, or 'unjust' provisions in contracts, with the purpose of avoiding 'unjust' consequences.[249] For the purposes of the Act, 'unjust' is defined to mean 'unconscionable, harsh or oppressive'.[250]

In determining whether a contract or contractual provision is 'unjust', a court must consider factors such as the inequality of bargaining power between the parties,[251] and the intelligibility of language used in the contract.[252]

Legislation dealing with misleading or deceptive conduct and misrepresentations

Section 18(1) of the ACL provides that 'A person must not, in trade or commerce, engage in conduct that is misleading or deceptive or is likely to mislead or deceive'.[253]

Section 29 of the ACL prohibits the making of false or misleading representations as to certain matters (listed in section 29(1)) in connection with 'the supply or possible supply of goods or services' or with the 'promotion by any means of the supply or use of goods or services'.[254]

As the 'conduct' covered by section 18 includes the making of statements[255] (and 'misleading or deceptive' does not have a meaning materially different from 'false or misleading'[256]), there is potential for overlap in the application of section 18 and section 29.

Both terms contained in contracts,[257] and statements made prior to entry into a contract,[258] may constitute conduct capable of breaching section 18.

In interpreting section 18, the ordinary meaning of the words should be applied to give the fullest relief allowable,[259] so that the provision has the potential to capture a broad range of conduct.[260] The terms 'goods' and 'services' are, as mentioned above, defined inclusively in the ACL,[261] and the

[249] *Contracts Review Act* s 7.
[250] *Contracts Review Act* s 4.
[251] *Contracts Review Act* s 9(2)(a).
[252] *Contracts Review Act* s 9(2)(g). See also Clapperton and Corones, see note 110, pp163-4.
[253] The text of the provision remains the same as in its predecessor, s 52 *Trade Practices Act 1974* (Cth).
[254] ACL s 29(1). The predecessor of the provision was s 53 *Trade Practices Act 1974* (Cth).
[255] Miller, see note 180, p1504.
[256] Miller, see note 180, p1646.
[257] Miller, see note 180, p1505. 'A breach of the terms of a contract may amount to a breach of ACL s 18. There is no reason in principle why a false statement in a contractual document cannot amount to misleading and deceptive conduct'. See also p1531.
[258] Miller, see note 180, p1531.
[259] Miller, see note 180, p1503.
[260] Miller, see note 180, p1503. Indeed, the Attorney-General's Department asserts that the prohibition is so broad that 'it can be raised in most situations involving a contractual dispute': Attorney-General's Department (Cth), *Contract law and consumer law* (24 October 2012). http://bit.ly/1UTMKLo
[261] ACL s 2.

expression ‘trade or commerce’, whilst requiring some connection to Australia, is otherwise broadly defined to include ‘any business or professional activity (whether or not carried on for profit)’.[262]

‘Puffery’ – exaggerated promotional statements – may in some circumstances be conduct falling under section 18.[263]

However, conduct will only be misleading or deceptive if the person to whom it is directed labours under an error (for example, a mistaken belief that an express representation is credible).[264]

[262] ACL s 2.

[263] Miller, see note 180, p1512.

[264] Miller, see note 180, p1510.

Improving the Communication of Privacy Information for Consumers