MARK ZUCKERBERG, THE COOKIE MONSTER – AUSTRALIAN PRIVACY LAW AND INTERNET COOKIES

ROBERT SLATTERY AND MARILYN KRAWITZ†

The internet has significantly increased the level of personal information that digital corporate entities can gather. These entities know everything from our current location, to the books we are interested in and where we plan to travel. Recent security leaks by Edward Snowden also revealed that both domestic and foreign governmental agencies can obtain information about us online. This raises important questions about the degree of privacy that Australians are entitled to while using the internet. This article aims to address some of these issues by analysing social media platforms using cookie technology within an Australian legal context. This article changes the debate on cookies by shifting the focus from online retailers to social media platforms. It also examines the new *Australian Privacy Principles* in the context of cookies.

I INTRODUCTION

How often are you logged into Facebook, whether on your laptop, tablet or smart-phone? Are you aware of the information that Facebook gathers about you? The answer to the second question is simple. Every internet website can track your every click, to gain knowledge about who you are, where you have been and where you are going. Internet service providers ('ISP')[1] gain this insight

† Marilyn Krawitz (LLB)(Dist)(UWA)(BBA)(Hon)(Schulich) is a lecturer at the University of Notre Dame Australia (Fremantle Campus), a lawyer and a PhD candidate. Robert Slattery (LLB)(Hon)(BA)(University of Notre Dame Australia) is a graduate solicitor.

1 For the purpose of this article, an Internet Service Provider ('ISP') refers to companies that provide a variety of services on the internet. This may include online retailers, social media providers and other e-commerce websites. It is not

through various data mining technology that enables them to infiltrate your inner secrets and create a detailed profile about you. One of these tracking mechanisms is a cookie that an ISP places on your computer. Big Brother is no longer a dystopian fantasy, but a reality. The cookie monster is real and he is watching you.

A private life is one of the foundations of liberal society. It is fundamental for the development of individualism, humour, uniqueness and the growth of a modern diverse society. It is necessary for the formation of intimate relationships because it allows a person to reveal parts of them that they may wish to keep from the rest of the world. It is a precondition for friends, individuality and love.[2] Warren and Brandeis first explained this notion of privacy in the American context in 1890 in their article *The Right to Privacy*.[3] Throughout this work, the authors observed that privacy related to the protection of confidential realms is a foundation of individual freedom in the modern age.[4] Warren and Brandeis believed that protection of privacy was essential as the government, press and corporations gain an increasing capacity to acquire previously inaccessible information.[5]

The purpose of this article is to analyse the increased encroachment upon individuals' privacy within the context of the internet. To achieve this, the article will look at the use of cookie technology by the social media platform Facebook. This approach

---

to be confused with companies that provide infrastructure to households that enable the use of the internet, such as Telstra, Optus or Vodafone.

2 Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (Vintage Books, 2001) 556; Stephen Davidson and Daniel Bryant, 'The Right of Privacy: International Discord and the Interface with Intellectual Property' (2001) 18(11) *The Computer & Internet Lawyer* 1, 7.

3 Arthur R Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers* (University of Michigan Press, 1971); William L Prosser, 'Privacy' (1960) 48 *California Law Review* 383, 384.

4 Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193, 196.

5 Ibid 206.

to cookies will be used because these platforms already raise multiple privacy concerns outside of data mining and cookies.[6]

There are over 1.06 billion users of Facebook with 618 million daily users and 680 million people who have Facebook mobile products.[7] The platform encourages users to disclose substantial amounts of personal information.[8] The platform's function is to allow users to create a digital profile about themselves. This profile contains a large amount of personal information, including: photos, a user's name,[9] where they are from[10] and places that they recently visited.[11] This 'profile style' makes it a magnet for personal and sensitive information from its users[12] by allowing users to create and publically articulate an online image.[13]

A user may create a Facebook account from the age of 13. This gives Facebook the capacity to engage users and gather data for an extensive time period.[14] As a result, Facebook can track a person's life from puberty, through their twenties until they have children and, potentially, until they die. This tracking capability enables Facebook to harvest and store detailed information about its users for a long period. Whilst these aspects of Facebook apply to some other social media, this article is using Facebook as a case study.

---

6 This can include the GPS locations of where messages were sent, locations where another user 'checked you in', photos of the individual and any other information that the individual disclosed in their Facebook account.

7 Facebook, *Annual Report 2012*, <http://investor.fb.com/secfiling.cfm?filingID=1326801-13-3>.

8 Alyson Leigh Young and Anabel Quan-Hasse, 'Privacy Protection on Facebook' (2013) 14 *Information and Communication Society* 479, 481.

9 This information is contained in the user's name and email address that can be disclosed on the platform.

10 This information is contained in the disclosure of the user's 'home town'.

11 This information is gathered from GPS capabilities on smart phones.

12 The definitions of personal information and sensitive information are contained in the *Privacy Act 1998* (Cth) s 6. They are discussed in detail below in section IV of this article.

13 Young and Quan-Hasse, above n 8.

14 Facebook, *How Old Do You Have To Be To Sign Up For Facebook*, <https://www.facebook.com/help/210644045634222>.

This article will ultimately argue that regulation is necessary to obtain express consent from users before any data is gathered and to compel websites to actively disclose data gathering practices. Requiring informed consent will empower users by informing them of tracking technologies such as 'third-party cookies'. Users must also have access to consumer or client profiles that have been created about them from gathered data.

Section II of this article will provide background information on the nature of privacy and how digital technology can infringe upon it. Section III will analyse how Australian law can assist individuals to maintain their privacy and discuss whether the protection afforded is sufficient. Section IV of the article will discuss legislation that is relevant to this issue in other countries. Section V will provide potential legislative solutions to the gaps in Australian privacy law.

This research is significant because it shifts the study of data mining practices from e-commerce websites (which have received considerable attention) to social media platforms (which arguably have not). This shift is important because social media platforms already obtain a large amount of personal information from users. The research is also important because foreign and domestic government agencies have started to access the data stored by websites such as Facebook.[15]

[15] Australian Broadcasting Channel, *NSA Breached Privacy Rules Thousands of Times, Leaked Documents Show*, 17 August 2013, ABC News, <http://www.abc.net.au/news/2013-08-17/despite-obama27s-promises2c-nsa-breached-privacy-rules/4893876;%20http://www.abc.net.au/news/2013-09-06/new-snowden-documents-say-nsa-can-break-common-internet-encrypt/4940138>; Glenn Greenwald and Ewen MacAskill, 'NSA Prism Program Taps in to user Data of Apple, Google and Others', *The Guardian* (online), 7 June 2013, <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.

II THE NATURE AND EXPECTATIONS OF PRIVACY

A *Why is Privacy Important?*

Many competing rationales that assert the existence of a right to privacy in modern society have emerged since the article by Warren and Brandeis in 1890.[16] These commentaries have predominately developed from an American background, making them intrinsically linked to 'American rights' such as the pursuit of happiness.[17]

Despite this American-centric approach, commentators have identified with the broader international audience by reconciling privacy with an individual's right to exercise certain fundamental liberties.[18] These liberties include that privacy is: a requirement for the ability to develop diverse and meaningful relationships;[19] a basic aspect of an individual's personality and integrity;[20] a precondition for human dignity and for retaining a person's uniqueness and autonomy;[21] and a necessary prerequisite for intimacy.[22] Thus privacy, whether couched in terms of American jurisprudence or a human right, is fundamental for society. It ensures that individuals have the requisite freedom needed to

---

16 Miller, above n 3; Prosser, above n 3, 384. For criticisms of complete privacy see Gary Gumpert and Susan Drucker, 'The Demise of Privacy in a Private World: From Front Porches to Chat Rooms' (1998) 8(4) *Communication Theory* 408, 418.

17 *Olmstead v United States*, 277 US 438, 478 43 (9th Ct, 1928).

18 Julie E Cohen, 'Copyright and the Perfect Curve' (2000) 53(6) *Vanderbelt Law Review* 1799; Lemi Baruh, 'Read at your own Risk: Shrinkage of Privacy and Interactive Media' (2007) 9 *New Media Society* 187, 190.

19 Ferdinand David Schomean (ed), *Philosophical Dimensions of Privacy* (Cambridge Press, 1984) 207, 292; Charles Fried, 'Privacy [a moral analysis]' (1968) 77 *Yale Law Journal*, 475, 485.

20 Fried, above n 19.

21 Edward J Bloustein, 'Privacy as an Aspect of Human Dignity: an Answer to Dean Prosser' (1964) 39 *New York University Law Review* 962.

22 Robert S Gerstein, 'Intimacy and Privacy' (1978) 89(1) *Ethics* 76.

develop and maintain individual thought, private relations and human dignity.[23]

The Control Theory of Privacy protects the privacy of individuals.[24] The central concept of the Control Theory is that individuals must be able to determine when, how, and to what extent information about them is communicated to others.[25] Privacy under this theory, and within the context of internet usage, becomes the freedom to develop an online digital persona while limiting the influence of others.[26]

Privacy is maintained when the individual can control the circulation of information relating to them.[27] The theory recognises the importance of individual autonomy and the significance of 'choice' that individuals should enjoy.[28] Choice has a fundamental

---

[23] The authors of this article agree that privacy is essential for individualism. This is not to say that there are no other reasons for protection (such as maintaining a power relationship): see Rosa Ehrenreich, 'Privacy and Power' (2001) 89 *The Georgetown Law Journal* 2047, 2053, 2060. Privacy will also often depend on context: see Robert McArthur, 'Reasonable Expectations of Privacy' (2001) 3 *Ethics and Information Technology* 123. However, a detailed discussion of competing philosophical rationales is beyond the scope of this article.

[24] M David Ermann, Mary B Williams and Claudio Gutierrez (eds), *Computers, Ethics and Society*, (New York, Oxford University Press, 1990) 51. This is believed to be the best approach to protect privacy within cyberspace. Full and complete discussion of the competing philosophical methods is beyond the scope of this article. This is because the article aims to provide a practical legislative solution to any gaps in the Australian legal context. For conceptual criticisms of the Control Theory and other theories see William Parent, 'Privacy: A Brief Survey of the Conceptual Landscape' (1995) 11(1) *Santa Clara Computer & High Technology Law Journal* 21, 22; Daniel Lin and Michael C Loui, 'Taking the Byte Out of Cookies: Privacy, Consent and the Web' [1998] *Ethics and Social Impact*, *ACM Policy* 39, 40; James Moor, 'Towards a Theory of Privacy in the Information Age' [1997] 27(3) *Computers and Society* 27, 30.

[25] Alan F Westin, *Privacy and Freedom* (Athenaeum Press, 1967).

[26] Niels van Dijk, 'Property, Privacy and Personhood in a World of Ambient Intelligence' (2010) 12 *Ethics and Information Technology* 57, 63.

[27] Arthur Miller, *The Assault on Privacy* (Harvard University Press, 1971) 25.

[28] Herman Tavani, 'Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy' (2007) 38(1) *Metaphilosophy* 1, 7.

requirement that a person enjoys full knowledge of what they are disclosing and how that information will be used.[29] Without this full knowledge, an individual's consent to the use or gathering of the information will not be adequate.

B *How does Digital Technology Infringe Upon Privacy?*

Modern technology and information gathering has changed society to a point where people exist in an environment of constant surveillance.[30] Details about their lives, interests, consumption patterns and other personal information are constantly gathered through a variety of data mining tools.[31] Entities controlling this data mining technology can then use this information to create patterns and correlations. By using complex algorithms, the correlated data can then be related to a user to categorise them into various 'types of persons' for targeted advertising.[32]

Through these classifications, and by combining separate sources of information, data controllers can create profiles to help predict the preferences of users.[33] The data controllers can then tailor products that a particular user is likely to accept.[34] These digitally created profiles then build presuppositions about individuals, creating self-enforcing feedback based on the user's behaviour.[35]

---

29 Ibid.

30 Baruh, above n 18; Gary Marx, *Undercover: Police Surveillance in America* (University of California Press, 1989).

31 Baruh, above n 18; Dustin Berger, 'Balancing Consumer Privacy With Behavioural Targeting' (2011) 27 *Santa Clara Computer and High Tech Law Journal* 4, 7; Gumpert and Drucker, above n 16, 415.

32 van Dijk, above n 26, 61.

33 Julie E Cohen, 'A Right To Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace' (1996) 28 *Connecticut Law Review* 981; Frank Franzak, Dennis Pitta and Steve Fritsche, 'Online Relationships and the Consumer's Right to Privacy' (2001) 18(7) *Journal of Consumer Marketing* 631, 637; Diane Michelfelder, 'The Moral Value of Informational Privacy in Cyberspace' (2001) 3 *Ethics and Information Technology* 129, 134.

34 W Lance Bennett and Robert M Entman (eds), *Mediated Politics: Communication and the Future of Democracy* (Columbia University Press, 2001) 141-59.

35 van Dijk, above n 26, 62.

This causes the user to react to the profile in a way that conforms to it, creating a self-enforced status of what is considered 'normal'.[36] This self-enforced data projection then creates an 'autonomy trap' in which an ISP can manipulate individuals into purchasing what they are more likely to accept rather than what they need based on an informed decision.[37] Cookies are one of these tools and are an essential part of data mining on the internet.[38]

A cookie is an invisible piece of information collection technology operating on the internet to gather data about users.[39] It consists of a small data file that is automatically downloaded onto a user's computer after that user has visited a website (assuming that the user does not turn cookies off on their computer).[40] The function of the cookie is to place a unique identifier on the computer so that the website can recognise and store information about the actions of the individual while on that website.[41] It records how the individual

---

36 Ibid.

37 Andrew McStay, 'I consent: An Analysis of the Cookie Directive and its Implications for UK Behavioral Advertising' (2013) 15 *New Media Society* 596, 599; Baruh, above n 18, 191; Tal Z Zarsky, '"Mine Your Own Business!": Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion' (2002) 5 *Yale Journal of Law & Technology* 1, 1-55.

38 There are other technologies that are important for the study of privacy in the information age. This includes technologies such as Cell-ID Positioning Technology ('CIPT'). CIPT use mobile phone signals between towers to determine the location of individuals. Companies can then use the location to text the individuals' advertisement of specials in that area. For further detail about this and similar technologies, see Francoise Gilbert, 'No Place to Hide? Compliance & Contractual Issues in the Use of Location-Aware Technologies' (2007) 11(2) *Journal of Internet Law* 3.

39 Senate Select Committee on Information Technologies, Parliament of Australia, *Cookie Monsters?: Privacy in the Information Society* (2000) 14.

40 Ibid.

41 David J Phillips, 'The Influence of Policy Regimes and the Development of Social Implications of Privacy Enhancing Technologies' (Paper presented at the Telecommunications Policy Research Council, 29th Research Conference on Communication, Information and Internet Policy, Alexandria, 27-29 October 2001); Baruh, above n 18, 200.

arrived at the website, what they did while there and what their ultimate destination was.[42]

Certain cookies can track internet users across a variety of different websites[43] through using specifically assigned identifying numbers.[44] This particular function of cookies is predominately performed by what are called 'third-party cookies'. These cookies are often placed on a website through advertisements, images or scripts that are hosted on a first party website by a third party server.[45] Third-party cookies do not require user interaction to be loaded on the individual's browser and are more persistent than other types of cookies.[46] The third-party cookie can be used to access different websites and internet sessions instead of a single visit.[47] As the name suggests, these cookies are often placed on a website by a separate organisation.

Cookies that have been stored on a person's computer can be accessed by them; however, the individual needs to be technologically literate to find them.[48] This feature makes cookies invisible trackers.[49] The cookie will give this information, without the individual's express consent, to the operators of the website and also to undisclosed third parties.[50] The practical effect is that cookies may access varying degrees of personal information

---

42 Baruh, above n 18, 195; Calin Gurau, Ashok Ranchod and Claire Gauente, '"To legislate or not to legislate": a comparative exploratory study of privacy/personalisation factors affecting French, UK and US Web sites' (2003) 20(7) *Journal of Consumer Marketing* 652, 660.

43 Senate Select Committee on Information Technologies, above n 39, 15.

44 Paul Lansing and Mark Halter, 'Internet Advertising and Right to Privacy Issues' (2003) 80 *University of Detroit Mercy Law Review* 181, 184.

45 Jo Pierson and Rob Heyman, 'Social Media and Cookies: Challenges for Online Privacy' (2011) 13(6) *Info* 30, 35.

46 Ibid.

47 Ibid.

48 Phillips, above n 41; Baruh, above n 18, 200.

49 Baruh, above n 18, 200.

50 Brian Pennington, 'New Technology Briefing: Cookies – Are They a Tool for Web Marketers or a Breach of Privacy?' (2001) 2(3) *Interactive Marketing* 251, 255.

without the user knowing that the information is being gathered, how it will be used or the implications for their privacy.

This function of cookies allows websites to save information about their users,[51] and gives marketers a 'dream opportunity to personalize their services'[52] through the creation of data mined profiles. Advertisers and ISPs can use this technology to track the movements and gather information about the users who visit the site to examine their personal preferences.[53]

The internet company DoubleClick provides an illustration of the use of tracking cookies.[54] DoubleClick's primary function is to place cookies on a large number of partner websites through using advertising banners. When a user visits one of these websites, DoubleClick's technology instantaneously reads the cookie saved on their hard drive and produces targeted advertisements based on the user's supposed preferences. The scope of this tracking is extensive, serving over 5.3 billion requests on more than 6,400 websites to deliver advertisements to over 48 million unique web users in December 1998 alone.[55]

Research has explored the use of cookies within the context of online retail websites. This includes the work of Caudill and Murphy[56] who assert that a website's use of cookies is an obvious

---

51 Rajiv Shah and Jay Kesan, 'Recipes for Cookies: How Institutions Shape Communication Technologies' (2009) 11 *New Media & Society* 315, 316.

52 Dave Chaffey and P R Smith, *eMarketing excellence: Planning and Optimizing Your Digital Marketing* (Butterworth-Heinemann, 3rd ed, 2008) 245.

53 Vincent Muller, 'Would You Mind Being Watched by Machines? Privacy Concerns in Data Mining' (2003) 23 *Artificial Intelligence and Society* 529, 533.

54 *Re DoubleClick Inc. Privacy Litigation*, 154 F Supp 497 (D NY, 2001). Accessible from <http://cyber.law.harvard.edu/is02/readings/doubleclick.html>.

55 Lansing and Halter, above n 44; Darren Charters, 'Electronic Monitoring and Privacy Issues in Business-Marketing: The Ethics of DoubleClick' (2002) 35 *Journal of Business Ethics* 243.

56 Eve Caudill and Patrick Murphy, 'Consumer Online Privacy: Legal and Ethical Issues' (2000) 19(1) *Journal of Public Policy and Marketing* 7.

violation of privacy. This violation occurs because the majority of consumers do not know that data is being collected or the means of collection.[57] To support their contention the authors provide a comparative example of digital commerce using a physical store location, such as Wal-Mart. The authors ultimately argue that people have greater control over their personal and private information within a physical store location.[58]

Like online retailers and advertisement agencies, Facebook uses cookie technology to deliver products, services and advertisements.[59] According to Facebook's privacy policy, the use of cookie technology enables the organisation to perform three main tasks: show 'what matters' to the user; improve the user's experience; and provide security to users.[60]

Facebook may place cookies when the user visits its platform or it may use third-party cookies when the user accesses a 'partner' website. The consequence is that Facebook cookies can send data back to Facebook when a user accesses different websites when they are not 'logged in' on Facebook or do not have an account. This provides Facebook with a wealth of personal information about its users which it can use to provide tailored advertisements.[61]

Privacy concerns relating to Facebook's use of cookies extend beyond direct market advertising to the use of data stored by domestic and foreign government agencies. Currently, Australian law provides protection from government access to data without

---

57 Ibid 13.

58 Ibid 14.

59 Facebook, *Cookies, Pixels & Similar Technologies: How Cookies Work*, <https://www.facebook.com/help/cookies>.

60 Ibid.

61 Pierson and Heyman, above n 45, 30; Facebook, *Cookies, Pixels & Similar Technologies: How Cookies Work*, <https://www.facebook.com/about/privacy/cookies>; Lauren Effron, 'Facebook Privacy Concerns: How to Protect Yourself', *ABC News* (online), 16 November 2011, <http://abcnews.go.com/blogs/technology/2011/11/facebook-privacy-concerns-how-to-protect-yourself/>.

requesting permission and the use of surveillance equipment. This is achieved through the *Telecommunications (Interception and Access) Act 1979* (Cth)[62], the *Telecommunications Act 1997* (Cth)[63] and the *Surveillance Device Act 2004* (Cth).[64] The protection that these Acts provide may change[65] as security concerns begin to outweigh the desire for individual privacy.[66]

This move away from privacy can be seen in the United States through the recent intelligence leak by Edward Snowden, a former National Security Agency ('NSA') sub-contractor. The disclosure by Snowden showed that a project labeled 'PRISM' enabled the NSA to have direct access to the databases of large internet companies (such as Facebook) that collect extensive amounts of personal and sensitive information.[67] This program allowed the NSA to acquire targeted communications without needing to request the information from the service providers or obtain court orders.[68] The PRISM project greatly affects Australians because it targets foreign nationals[69] and any data gathered can be shared with

---

62 This Act prohibits the interceptions of communications over telecommunication systems as well as access to stored information except where authorised. This can include emails, SMS and voicemails.

63 Part 13 of this Act (Protection of Communications) places an obligation on telecommunication to protect the privacy of people unless disclosure is required in special circumstances.

64 This Act regulates the use of surveillance devices by law enforcement agencies.

65 Rebecca Le May, 'Privacy Fears as Surveillance Law Reviewed', *The Australian* (online), 2 August 2012, <http://www.theaustralian.com.au/news/breaking-news/privacy-fears-as-surveillance-law-reviewed/story-fn3dxiwe-1226423605766>.

66 Detail about this balance is beyond the scope of this article. For further information, see Marc van Lieshout et al, 'Reconciling Privacy and Security' (2013) 26(1) *Innovation: The European Journal of Social Science Research* 119.

67 Greenwald and MacAskill, above n 15.

68 Ibid.

69 Director of National Intelligence, *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (8 June 2013), <http://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf>.

Australian governmental departments (such as ASIO) to bypass domestic protection.[70]

Similar to the executive branch of government, the judiciary has begun to use subpoenas to facilitate the use of stored data by ISPs in court proceedings. This occurred in *United States v Rigmaiden*,[71] where investigators successfully tracked IP addresses in emails between a hacker (Rigmaiden) and two confidential informants. The IP addresses were registered to Verizon (an American telecommunications company) and the prosecution had to acquire the data by a subpoena.[72] It can be reasoned from this that Australian prosecutors may be able to acquire location data, such as the information contained in Facebook's 'checked in' functions. More pressing for the purpose of this article is *People v Harris*,[73] where a subpoena was issued to Twitter, another social media website, for subscriber information and stored communications. While these are American decisions, they might provide a persuasive precedent for Australian courts to follow in relation to stored data. Given Australians' substantial use of social media, it is likely that a similar case will come before Australian courts in the future.

The use of subpoenas is fast becoming an important tool to obtain general-purpose data for judicial proceedings.[74] While the use of subpoenas is beyond the general nature of this article, it is an

---

70 Such intelligence trading agreements can occur under the *UKUSA Agreement* 1956. The agreement can be accessed from <http://www.nsa.gov /public_info/_files/ukusa/new_ukusa_agree_10may55.pdf>; Department of Defence and Security, Australian Government, *UKUSA Allies* <http://www.dsd.gov.au/partners/allies.htm>. Details about this alliance and how intelligence is shared are beyond the scope of this article.

71 *United States v Rigmaiden* (D Ariz, No CR 08-814-PHX-DGC, 8 May 2013).

72 Ibid 35.

73 *People v Harris* 949 N.Y.S.2d 590 (2012).

74 Andrew Crocker, 'Trackers That Make Phone Calls: Considering First Amendment Protection For Location Data' (2013) 26(2) *Harvard Journal of Law & Technology* 620, 633.

important consideration about how people may use information stored by ISPs.[75]

III AUSTRALIAN LEGAL PROTECTION

A *The Common Law*

Australian Broadcasting Commission v Lenah Games Meats Pty Ltd[76] allowed for Australian courts to potentially adopt a common law right to privacy. However, whether Australian courts recognise a tort for the breach of privacy is still unclear.[77] In the Queensland District Court decision *Grosse v Purvis*,[78] Skoien J found that such a tort existed in Australia. In *Kalaba v Commonwealth*,[79] Heerey J thought that the weight of authority was against the existence of a common law right to privacy.[80] In *Dye v Commonwealth Securities Limited* Katzmann J stated:

> I accept, therefore, that it would be inappropriate to deny someone the opportunity to sue for breach of privacy on the basis of the current state of the common law, although whether the matters complained of in the present case would be actionable if a tort of privacy were recognised is another question.[81]

In *Maynes v Casey*, Basten JA stated that certain cases 'may well lay the basis for development of liability for unjustified intrusion on personal privacy'.[82]

---

[75] The use of subpoenas and data is beyond the scope of this article. For more information see Joshua Gruenspecht, '"Reasonable" Grand Jury Subpoenas: Asking For Information in the Age of Big Data' (2011) 24(2) *Harvard Journal of Law & Technology* 543.

[76] (2001) 208 CLR 199.

[77] *Chan v Sellwood* [2009] NSWSC 1335, [37].

[78] (2003) Aus Torts Reports 81-706.

[79] [2004] FCA 763.

[80] *Gee v Burger* [2009] NSWSC 149, [53].

[81] [2010] FCA 720, [290].

[82] *Maynes v Casey* [2011] NSWCA 156, [35].

It is evident from other jurisdictions, such as the United Kingdom and New Zealand, that any protection that the common law would provide could not provide users with sufficient control over their personal information. This is because the action is better suited to situations where a plaintiff suffers actual harm. It would therefore encompass situations analogous to a celebrity being photographed outside of a narcotics anonymous centre.[83] The common law would not enable the public as a whole to control the level of information that ISPs gather.

B *The Privacy Act 1988* (Cth)

The *Privacy Act 1988* (Cth) ('*Privacy Act*') is a 'principle-based' regulation regime.[84] It relies on general maxims to articulate outcomes that regulate entities within society.[85] The scheme creates a system of express norms instead of detailed rules that create fundamental obligations which must be observed.[86] The purpose of a principle-based approach is to shift regulation from a process regime to one that focuses on outcomes. This approach allows organisations to make their own decisions within the regulatory framework to fit their business model.[87]

Principle-based regulation attempts to solve some of the problems associated with traditional regulation by allowing greater levels of flexibility.[88] This enables society to respond to new issues

---

83 *Campbell v Mirror Group Newspapers Ltd* (2001) 62 IPR 231; for a New Zealand example see *Hosking v Runting* [2004] NZCA 34 or *P v D and Independent News Auckland* [2000] 2 NZLR 591.

84 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth), 217.

85 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) vol 1, 234.

86 Julia Black, 'Principles Based Regulation: Risks, Challenges and Opportunities' [2007] *London School of Economics and Political Science* 3; Julia Black, 'Making a Success of Principles-Based Regulation' [2007] *Law and Financial Markets Review* 191, 192.

87 Australian Law Reform Commission, above n 85.

88 Ibid.

without creating new rules.[89] The principle-based approach can be contrasted with a rules-based regulation system. These standard rules are easier to interpret and set a minimum standard of compliance, but are less adaptable to changing circumstances.[90] By encouraging a flexible approach organisations can recognise the advantages of good information gathering practices. A more flexible style of regulation is considered more effective in managing technology-based enterprises.[91]

The principles relating to the use of personal and sensitive information are contained in schedule 1 of the *Privacy Act* and are referred to as the Australian Privacy Principles ('APP').[92] There are thirteen APPs that require organisations which collect personal or sensitive information to do so by lawful and fair means. Under these APPs, organisations can only collect personal information in a method that is not intrusive and is necessary for the organisation's functions or activities.[93] The collection of 'sensitive information' is treated differently from personal information and requires the organisation to obtain the consent of the individual before gathering the information.[94] Personal information is defined in section 6 of the *Privacy Act* to include information about an individual that can be used to identify them.[95] This definition raises questions about whether it would include data processing techniques, such as cookie technology, that only ascertain an IP address as opposed to an 'identity'.

To assist in interpreting this definition, a number of submissions were made to the Senate Legal and Constitutional References

89 Black, Principles Based Regulation, above n 86, 8.
90 Black, Making a Success of Principles-Based Regulation, above n 86, 193-194.
91 Investment and Financial Services Association, *Towards Better Regulation: Policy on Future Regulation of Financial Services in Australia* (2006) 3; Australian Law Reform Commission, above n 85, 236.
92 *Privacy Act 1988* (Cth) sch 1 ('APP').
93 Ibid APP 3.
94 Ibid.
95 *Privacy Act 1988* (Cth) s 6(1); Australian Law Reform Commission, above n 85, 294.

Committee.[96] The submissions commented that the definition contained in section 6(1) of the *Privacy Act* would not cover data gathering processing techniques[97] because these technologies contain information that is not necessarily linked to the user's identity.[98] If this interpretation is endorsed, then the scope of the *Privacy Act* information will become problematic when applied to cyberspace.[99]

The office of the Privacy Commissioner does not agree with this interpretation and narrow application of the APPs. Instead, the Privacy Commissioner:

> recognises the challenges posed by the development of new technologies and processes, particularly in the field of data-matching, that have the potential to create identified information from data sources containing previously anonymous data. However, the definition of personal information leaves open the flexibility to consider the degree to which an organisation is able to 'reasonably ascertain' someone's identity, including by the use of such technologies.[100]

From this it can be reasoned that the information extracted by cookies from individuals will likely be classified as personal information. This technological based approach to the definition of 'personal information' is supported by current loose-leaf

---

96 Senate Select Committee on Information Technologies, above n 39.

97 Cookies are an example of a data gathering technique.

98 Senate Legal and Constitutional References Committee, Parliament of Australia, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [3.19]-[3.24]; Electronic Frontiers Australia Inc., *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 24 February 2005; Australian Privacy Foundation, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 1 March 2005; Centre for Law and Genetics, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 1 February 2005 as submitted to the Senate Select Committee on Information Technologies, above n 39.

99 Graham Greenleaf, 'Privacy principles—irrelevant to cyberspace?' (1996) 3(3) *Privacy Law and Policy Reporter* 115, <http://www2.austlii.edu.au/itlaw/articles/IPPs.html>.

100 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Law Reform Commission, above n 85, 278.

services.[101] Sensitive information is defined in section 6 of the *Privacy Act* to include any information about an individual's

> racial or ethnic origin, political opinions, membership of political associations, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, health information or other genetic information.[102]

Cookies have the ability to collect data from any source in which they are placed. This will include websites that disclose a person's racial or ethnic origin, religious belief, financial identity or status. Due to the vast level of information present on the internet, the cookie can collect sensitive information and personal information.

The third APP requires that an organisation only uses and discloses sensitive information with the consent of the individual.[103] The organisation must take reasonable steps to ensure that the personal information that it handles is complete and up to date[104] and must protect that information from misuse and loss.[105] It must also take steps to destroy or permanently 'de-identify' personal information if it is no longer needed.[106]

Whether individuals have consented to the use of any sensitive information that has been gathered by an organisation is a serious concern with this APP.[107] The *Privacy Act* defines 'consent' as either express or implied.[108] Express consent is apparent when a person makes an informed decision to give their voluntary agreement to any data collection.[109] Implied consent, on the other

---

[101] LexisNexis Butterworths, *Law of eCommerce* (at 26 February 2013).
[102] *Privacy Act 1988* (Cth) s 6(1).
[103] Ibid APP 3.
[104] Ibid APP 10.
[105] Ibid APP 11.
[106] Ibid APP 4.
[107] It should be noted that the APP's do not require consent for the collection of personal information.
[108] *Privacy Act 1988* (Cth) s 6(1).
[109] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth), 54.

hand, depends entirely on circumstance.[110] These provisions do not alter the general law requirements of consent[111] incorporating the need for it to be voluntary and for the individual to understand what they are consenting to.[112] This accords with the Australian Law Reform Commission's interpretation of consent which states that to give the requisite consent a person must be fully informed and aware of what they agree to.[113]

This definition raises some concerns. Firstly, it would seem illogical that consent can be given to an action after it has already occurred. In spite of this logic, the consent definition in the *Privacy Act* does not require an organisation or ISP to obtain consent before they use cookie technology. This is because its use will fall under the all-embracing definition of implied consent. This is evident from Facebook using cookie technology before a user has had the time to read the privacy policy. It is further evident from Facebook using third-party cookies, placed on their 'partner websites', to gather information about users who are not logged into Facebook or who do not have a Facebook account. This allows Facebook to obtain information without the user knowing.[114]

It can be extracted from common law principles that consent may have a degree of flexibility about the scope of sensitive information that can be collected. Thus, an organisation may be able to extract sensitive information of a certain type of category, within the 'rules' that an individual has consented to, which may infringe upon another category that they have not consented to. For example, a person may consent to an organisation knowing that they have a

---

110 Ibid.

111 Australian Law Reform Commission, above n 85, 669 quoting Douglas-Stewart, *Annotated National Privacy Principles* (3rd ed, 2007).

112 Ibid.

113 Ibid.

114 Facebook, *How Do Third Parties Use Cookies, Pixel Tags ("Pixels") and other Similar Technologies on Facebook,* <http://www.facebook.com/help/159967110798373>; Samantha Felix, 'How to Stop Facebook from Tracking You', *Business Insider* (online), 12 September 2012, <http://www.businessinsider.com.au/heres-how-to-stop-facebook-from-tracking-you-2012-9?op=1>.

political affiliation with 'marriage equality' groups, but may not have consented to that organisation knowing that they are gay. This gives data collection agencies the ability to obtain a larger amount of information than if the definition of consent was narrower. Data collection agencies would likely argue that the consent that an individual provides can be applied broadly.

This definition of consent contained in the *Privacy Act* can be contrasted with the *European Union's Directive 95/46/EC*.[115] Article 8 of this Directive defines consent as 'any freely given specific and informed indication of his wishes but which the data subject signifies his agreement to personal data relating to him being processed'.[116] The inclusion of the words 'specific and informed' narrows the scope of the consent that needs to be given. This adds clarity to the law and the arguments that may arise regarding the scope of consent that an individual gives. The British Information Commissioner highlighted that the definition excludes consent being acquired after the use of cookies occurred.[117]

Another requirement of the APPs is that organisations must inform individuals of the purpose of the collection of their information.[118] Organisations must also give access to the information held about them unless an exception applies.[119] Organisations must have implemented a written privacy policy that states how they will manage the personal information.[120] A written privacy policy would be a helpful tool for outsiders to understand an organisation's approach to privacy. The flexibility that is

---

[115] *Directive 95/46/EC of the European Parliament and of the Council 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* OJ L 281, 23/11/1995.

[116] Ibid art 8.

[117] Information Commissioner's Office, *Privacy and Electronic Communications Regulations: Guidance on the Rules on Use of Cookies and Similar Technologies* (May 2012) Information Commissioner's Office, <http://www.ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies>.

[118] Ibid APP 5.

[119] Ibid APP 12.

[120] Ibid APP 1.

permissible under the principle-based regime allows these organisations to determine the level of information that is given to protect their marketing and profit based interests.

If an organisation has a person's personal information, it can only use it for direct marketing if the person 'would reasonably expect the organisation to use or disclose the information for that purpose'.[121] An exception to this is if the organisation has received the consent of the individual.[122] If an ISP gives an individual's personal information to someone outside Australia, the organisation must take reasonable steps to ensure that the person or organisation overseas follows the APPs.[123] The purpose of this requirement is to prevent direct marketing practices by organisations. The principle is not concerned with the collection and storage of personal information by organisations by data gathering technologies. Similar issues concerning the definition of consent are present under this requirement because it is difficult to define the scope of the consent given and also whether that consent is truly informed.

An action that infringes one of the APPs or approved privacy policies is an interference with a person's privacy.[124] An individual may lodge a complaint with the Privacy Commissioner about the alleged interference[125] which will grant the Commissioner the authority to investigate the action.[126] The Commissioner can also investigate an act or practice independently that they believe may interfere with an individual's privacy.[127]

Before commencing an investigation the Commissioner must inform the respondent about the enquiry.[128] The investigation can

[121] Ibid APP 7.
[122] Ibid.
[123] Ibid APP 8.
[124] Ibid s 13.
[125] Ibid s 36.
[126] Ibid s 40.
[127] Ibid s 40(2).
[128] Ibid s 43(1).

be conducted as the Commissioner deems appropriate.[129] The Commissioner can obtain information and documents,[130] and examine witnesses under oath or affirmation.[131] The Commissioner may call a compulsory conference. At this conference the Commissioner can direct the complainant, the respondent, and any other person to attend.[132] If they do not attend, then they will be liable to pay either a $1,000 fine or face six months imprisonment or both.[133]

After an investigation, the Commissioner may either dismiss the complaint or find that the claim is substantiated. The Commissioner may then make a determination that can include: (1) a declaration that the respondent has engaged in conduct constituting an interference with the privacy of an individual; (2) a declaration that the respondent should perform an act to redress the damage suffered (including damage to feelings or humiliation); or (3) a declaration that the complainant is entitled to compensation.[134] If the respondent does not follow the declaration, then the Commissioner may bring an action in the Federal Court or Federal Circuit Court.[135]

The Commissioner may assess organisations' compliance with the APPs.[136] They may also inform organisations that they must complete a privacy impact assessment. The privacy impact assessment is a written document that states the effect that an organisation's actions may have on people's privacy and suggests ways to minimise it.[137]

[129] Ibid s 43(2).
[130] Ibid s 44.
[131] Ibid s 45.
[132] Ibid s 46.
[133] Ibid s 46.
[134] Ibid s 52.
[135] Ibid s 55A.
[136] Ibid s 33C.
[137] Ibid s 33D.

The Commissioner can accept undertakings from organisations to take specific actions or not to take certain actions in relation to privacy.[138] The Commissioner can apply to the Federal Court or the Federal Magistrates Court to force an organisation to follow the undertaking or pay compensation because their failure to follow the undertaking caused loss or damage.[139] If an organisation causes 'serious and repeated interferences with privacy', then it may face a civil penalty.[140] In this case, the Commissioner may apply to the Federal Court or the Federal Magistrates Court for orders compelling the organisation to pay the civil penalty to the Commonwealth.[141] The Commissioner can only deal with issues that they have the jurisdiction to hear. So, while there appears to be quite stringent penalties for breaching APPs, the penalties may become somewhat redundant because they do not deal directly with the use of cookies.

C *Does the Privacy Act Provide Adequate Protection?*

To reiterate, Facebook, its affiliates and third parties use cookie technology to deliver targeted products, services and advertisements.[142] Facebook can place these cookies on a user's computer when they visit Facebook's platform or a partner website which permits the placement of third-party cookies. This tracking can occur if a person does not have an account or if they are logged out of their account.[143]

A preliminary enquiry must be made into whether Facebook collects 'personal' or 'sensitive' information about users within the definitions provided for in the *Privacy Act*.[144] As Facebook uses cookie technology in conjunction with 'third parties and other

[138] Ibid s 33E.
[139] Ibid s 33F.
[140] Ibid s 13G.
[141] Ibid s 80W.
[142] Facebook, *Cookies, Pixels & Similar Technologies: How Cookies Work*, <https://www.facebook.com/help/cookies>.
[143] Ibid.
[144] *Privacy Act 1988* (Cth) s 6.

parties', including when a user is logged off, it is likely that the site can obtain significant amounts of both types of information. To gather data about users, Facebook needs their 'consent', because the information will inevitably include sensitive information.

It is arguable that in providing a detailed privacy policy accessible to its users, Facebook has gained both implied and express consent to use cookies. However, this argument is weakened by the policy changing often and using a large amount of ambiguous language. This can be observed from the use of the words 'third parties and other partners', which produces a broad definition of who uses cookies. The Australian Information Commissioner raised this issue in May 2012,[145] but Facebook easily dismissed these concerns because the company would have to disclose an unreasonable level of information.[146] The effect of this is that, under the current *Privacy Act* provisions, organisations can place third-party cookies onto an indeterminable amount of websites. This is because the ISPs can use broad language and the APPs use a flexible principle-based approach to obtain implied consent.

[145] Office of the Australian Information Commissioner, *Changes to Facebook's Data Use Policy: Submissions to Facebook* (May 2012) Australian Information Commissioner, <http://www.oaic.gov.au/news-and-events/submissions/privacy-submissions/changes-to-facebooks-data-use-policy>; Office of the Australian Information Commissioner, *Correspondence: Facebook's data Use Policy Response* (30 July 2012) Australian Information Commissioner, <http://www.oaic.gov.au/news-and-events/statements/privacy-statements/changes-to-facebooks-statement-of-rights-and-responsibilities-and-data-use-policy/correspondence-facebook-s-data-use-policy-response>.

[146] Office of the Australian Information Commissioner, *Changes to Facebook's Data Use Policy: Submissions to Facebook* (May 2012) Australian Information Commissioner, <http://www.oaic.gov.au/news-and-events/submissions/privacy-submissions/changes-to-facebooks-data-use-policy>; Office of the Australian Information Commissioner, *Correspondence: Facebook's data Use Policy Response* (30 July 2012) Australian Information Commissioner, <http://www.oaic.gov.au/news-and-events/statements/privacy-statements/changes-to-facebooks-statement-of-rights-and-responsibilities-and-data-use-policy/correspondence-facebook-s-data-use-policy-response>.

Another issue about whether Facebook gained the requisite consent is defining the scope of the data that can be gathered from cookies. Facebook's privacy policy, in defining the scope of data that is gathered, refers only to a broad term of 'information'.[147] This term does not address the potential amount and detail of data that cookies can obtain from a vast number of websites that requires a more narrow definition of 'information'. The definition should make certain exclusions of websites including those that contain material relating to health, finances or religion. It should also exclude data such as email addresses, items purchased or credit cards used. Issues are also present about whether the individual truly gave their informed consent to the use of third-party cookies on Facebook's partner websites. A user may not be aware that they are being tracked by external third party entities when they are searching the web. This poses an issue for both young and older generations who may not be aware or technologically savvy.

The APPs require users to be able to access the personal and sensitive information stored by organisations; a requirement recognised by the Control Theory of Privacy. Facebook does allow users to access information stored by the website. This information can be obtained through the user's Facebook account, 'Activity Log' or by downloading an information file.[148] The Facebook account provides all information that a user has posted including photos, locations that the user has been 'tagged in', and messages sent through Facebook's private messaging function. The Activity Log is a tool that allows users to manage what they share on Facebook and are organised by the date that the events occur on Facebook.[149] The 'downloaded information' tool contains the same

[147] A similar analysis has been made of a variety of privacy policies to find ambiguities. See Jan Fernback and Zizi Papacharissi, 'Online Privacy as Legal Safeguard: The Relationship Among Consumer, Online Portal and Privacy Policies' (2007) 9 *New Media Society* 715, 724.

[148] Facebook, *Accessing Your Facebook Data,* <https://www.facebook.com/help/405183566203254>.

[149] Facebook, *Explore Your Activity Log,* <https://www.facebook.com/help/www/437430672945092>.

information that is provided on the user's Facebook account and Activity Log in a downloadable file.[150]

The information that users can obtain from these tools includes IP addresses that cookies gathered.[151] This is presented to the user in a complex numerical form. The information does not tell the user what the specific data from the cookies are or how it is relevant to Facebook's functions. This downloaded information tool does not allow users to access, control or delete the cookie data that Facebook has gathered. This falls short of the Control Theory of Privacy because of the complexity of the information that is presented to users. It does not allow access to the client or consumer profile that the ISP has created.

APPs seven and eight are relatively new.[152] APP seven deals with the use of personal information by regulating direct marketing practices. In this regard, it indirectly affects the way that organisations can use the information that has been gathered by cookies. However, the amendments still fail to expressly regulate the use of cookie technology to gather information about internet users.

It can be concluded that the *Privacy Act* does not adequately regulate the uses of cookie technology by websites such as Facebook. These websites can use broad and ambiguous privacy policies to control and access individuals' personal and sensitive information. The legislation attempts to deal with some of the uses of the information stored rather than dealing with the method in which it is obtained. The overall affect is that privacy under the *Privacy Act* does not reach the minimum threshold of privacy protection that the Control Theory requires, because sites such as Facebook are able to use cookie technology without obtaining

[150] Facebook, above n 148.
[151] Ibid.
[152] They came into effect in March 2014. See *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth).

informed consent or allowing access to the personal information that is stored.

IV SOLVING THE PROBLEM

It's clear that there are problems with the Australian legislative framework to provide an appropriate degree of privacy protection to Facebook users. This section attempts to find potential solutions to this problem by analysing two different methods of privacy regulation that are used internationally. The first is the United States' approach of market self-regulation. The second is the European Union's use of legislation.[153] The overall argument of this section is that an increase in self-regulation will be ineffective to provide privacy protection to online users. Australians would benefit from increased legislation that allows users to access and control the information on the internet.

A *The United States and Self-Regulation*

Digital privacy issues in the United States first received attention in 1996 when an investigation headed by Ira Magaziner issued a report entitled: *A Framework for Global Electronic Commerce (Draft Report).*[154] The report noted a need to protect consumer privacy for electronic commerce to reach its full potential.[155] It recommended a self-regulatory system whereby competition and consumer choice would shape the degree of protection.[156]

---

[153] These are not the only jurisdictions with privacy laws in place but are the focus of this article: see, eg, Surya Deva, '"Yahoo! For Good" And the Right To Privacy of Internet Users: A Critique' [2008] *Journal of Internet Law* 3, 4-5 and her analysis of Hong Kong's privacy laws.

[154] Joseph Regale, *A Framework for Global Electronic Commerce* (1997) World Wide Web Consortium, <http://www.w3.org/TR/NOTE-framework-970706>.

[155] Elizabeth Blumenfeld, 'Privacy Please: Will the Internet Act to Protect Consumer Privacy Before the Government Steps In?' (1998) 54 *The Business Lawyer* 349, 368; Regale, above n 154.

[156] Blumenfeld, above n 155.

Self-regulation is not the same as a 'pure market' solution. Instead, the industry develops rules and enforcement mechanisms through independent regulatory bodies to substitute for government regulation.[157] For this system to be effective, organisations need to voluntarily adopt and implement privacy policies that conform to an industry set level of privacy protection.[158] This makes user privacy a commodity and the categories of information protected become determined by free-market forces.[159] This can have the potential to place what is protected into narrowly defined categories of sensitive data (such as financial or medical information).[160] Self-regulation also assumes that individuals are rational economic agents who can make informed decisions regarding the protection or divulgence of personal information.[161] It is espoused under this theory that the government should not put excessive restrictions on electronic commerce and the internet should be driven by the market, as opposed to regulation.[162]

Commentators argue that legislation may confuse consumers and give them a false sense of security about the enforceability of their rights.[163] Any increase in government regulation would further disrupt the free flow of consumer information that allows companies to provide society with better products and services.[164] Further, any additional government regulation could make electronic commerce more time consuming for consumers.

---

[157] Mary Caulnan and Robert Bies, 'Consumer Privacy: Balancing Economic and Justice Considerations' (2003) 59(2) *Journal of Social Issues* 323, 333.

[158] Ibid.

[159] Laurence Ashworth and Clinton Free, 'Marketing, Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns' (2006) 67(2) *Journal of Business Ethics* 107, 109.

[160] Ibid.

[161] Curtis Taylor, 'Consumer Privacy and the Market for Customer Information' (2004) 35(4) *RAND Journal of Economics* 631, 634, 638; Franzak, Pitta and Fritsche, above n 33, 634.

[162] Regale, above n 154.

[163] Caudill and Murphy, above n 56, 11.

[164] Ibid.

Self-regulation as a system of dealing with consumer privacy issues was fully implemented in 1999 under the Clinton Administration. The Federal Trade Commission ('FTC') understood that self-regulation was the least intrusive and most efficient means to ensure fair information practices online, given the rapidly evolving nature of the internet and computer technology.[165]

TRUSTe is an independent third party that provides an industry standard of self-regulation.[166] TRUSTe is a non-profit privacy body that places a 'stamp' on websites to signal to users that the organisation practices safe data-gathering and distribution processes.[167] The TRUSTe logo does not guarantee the privacy of an individual, rather it ensures that websites provide a fair disclosure of their information collection and data-mining practices.[168] Sites that break the policy have no specific retribution outside of harmful publicity.[169]

TRUSTe, as an example of self-regulation, does not provide the requisite level of privacy protection that the Control Theory of Privacy requires. This is because merely disclosing that an organisation observes fair information practices and, even when

---

[165] Martha Landesberg et al, *Privacy Online: A Report to Congress* (June 1998) Federal Trade Commission, <http://www.ftc.gov/reports/privacy3/priv-23a.pdf>; Martha Landesberg and Laura Mazzarella, *Self-Regulation and Privacy Online: A Report to Congress* (July 1999) Federal Trade Commission, <http://www.ftc.gov/os/1999/07/privacy99.pdf>; Federal Trade Commission, Online Profiling: A Report to Congress (2000) <http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf>.

[166] Information about TRUSTe can be accessed from its website <http://www.truste.com/>. For further examples see Janice Sipior, Burke Ward and Nicholas Ronigone, 'Ethics of Collecting and Using Consumer Internet Data' [2004] *Information Systems Management* 58, 64.

[167] Milena Head and Khaled Hassanein, 'Trust in e-Commerce: Evaluating the Impact of Third-Party Seals' (2002) 3(3) *Quarterly Journal of Electronic Commerce* 307, 324 <http://www.business.mcmaster.ca/is/Head/Articles/Trust%20in%20e-Commerce%20Evaluating%20the%20Impact%20of%20Third-Party%20Seals.pdf>; See also TRUSTe, *Privacy Program Requirements*, <http://www.truste.com/privacy-program-requirements/>.

[168] Fernback and Papacharissi, above n 147, 721.

[169] Ibid.

combined with strong internal controls, does not address concerns relating to trust and privacy.[170] It does not provide adequate disclosure or access to information. The limited effectiveness of TRUSTe is an example of a market-based approach that shows that self-regulation can be largely ineffective.[171]

There are three main reasons for this ineffectiveness. Firstly, users are unaware of the 'value' of their personal information to internet service providers.[172] As a result of this information asymmetry, individuals are no longer considered rational economic actors. Secondly, online users are unaware of how information is being gathered about them and how to prevent this from occurring.[173] This is particularly evident from the use of third-party cookies by Facebook to gather information from 'partner websites'. Thirdly, the lack of knowledge about information collecting technologies creates collective norms that do not reflect the true value of privacy.[174] This creates self-enforcing standards that corporations set, rather than the community.

Kathleen Kubis argues that internet companies exist in a regulatory realm of their own because of the internet's permeable digital and jurisdictional borders.[175] To mitigate against this anarchy, Kubis recommends the enactment of detailed legislation that gives privacy protection to electronic communication.[176]

---

[170] Caulnan and Bies, above n 157.

[171] Ibid.

[172] Francois LeSieur, 'Regulating Cross-Border Data Flows and Privacy in the Networked Digital Environment and Global Knowledge Economy' (2012) 2(2) *International Data Privacy Laws* 93, 102.

[173] Ibid.

[174] Ibid.

[175] Kathleen Kubis, 'Google Books: Page by Page, Click by Click, Users Are Reading Away Privacy Rights' (2011) 13 *Vanderbilt Journal of Entertainment & Technology Law* 217, 250.

[176] Ibid. See also Berger, above n 31, 56.

The FTC has noted the weakness of self-regulation. It states that the initiatives fell far short of expectations.[177] It acknowledged that self-regulation has been slow to provide sufficient privacy protection.[178] The FTC recommended legislative action that requires websites to provide notice, choice, access and security to users.[179] The FTC hopes that any proposal will prompt the industry into action.[180] Nevertheless, no legislative action has yet taken place.[181]

B *The European Union Legislative Approach*

Politicians in the European Union passed legislation that ensures the free movement of information while maintaining a high level of privacy protection.[182] The European directives were formulated in response to developments in information technology, and telecommunication networks in the European Union.[183] The directives impose stringent obligations on organisations to obtain fully informed consent before using cookie technology.

---

[177] Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress*, 35 <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>.

[178] Ibid 3.

[179] Baidie Farah and Mary Higby, 'E-Commerce and Privacy: Conflict and Opportunity' [2010] *Journal of Education for Business* 303, 305.

[180] Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress*, 35 <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>.

[181] Miriam Metzger and Sharon Docter, 'Public Opinion and Policy Initiative for Online Privacy Protection' [2003] *Journal of Broadcasting & Electronic Media* 350, 359. Sim Stiken and Nancy Roth argue that legislative remedies lead to a decrease in trust in a relationship. Their work has not been directly referred to as it deals predominately with the physical world as opposed to the digital one. For further detail see Sim B Stikin and Nancy L Roth, 'Explaining the Limited Effectiveness of Legalistic "Remedies" for Trust/Distrust' (1993) 4(3) *Organization Science* 367.

[182] Senate Select Committee on Information Technologies, above n 39, 47.

[183] Ibid; Gurau, Ranchod and Gauente, above n 42, 654.

The European Union position is evident in the *ePrivacy Directive 95/46/EC*[184] (recently amended *by Directive 2009/136/EC the 'Cookie Directive'*).[185] Article 5(3) of the *ePrivacy Directive* requires all member states to:

> Ensure that in the storing of information, or the gathering or access to information already stored, in the terminal equipment of a subscriber or user is only allowed on the condition that the subscriber or user concerned *has given* his or her *consent, having been provided with clear and comprehensive information*, in accordance with Directive 95/46/EC, inter alia about the purposes of the processing'.[186] [Authors' emphasis]

A major aspect of article 5(3) is the need to obtain consent before using cookie technology. To assist in defining and clarifying the term 'consent' within the European Union, the Article 29 Working Party released a document entitled, *Opinion 15/2011 on the Definition of Consent.*[187] The Working Party outlined two core issues that arise when considering 'consent' and cookies: the consent must be obtained before the cookie is placed and the information is stored; and the consent can only be obtained if information about the use of cookies has been given to the user.[188]

---

[184] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector* [2002] OJ L 201/37.

[185] *Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and User's Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on the Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws* [2009] OJ L 337/11.

[186] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector* [2002] OJ L 201/37 art 5(3).

[187] McStay, above n 37, 604.

[188] Article 29 Working Party set up under Article 29 of Directive 95/46/EC, *Opinion 15/2011 on the Definition of Consent* (adopted on 13 July 2011), 13. Accessible from <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf>.

This interpretation of consent endorses the view that it is difficult to obtain approval for an act after it has already occurred.[189]

To fulfil this definition of consent, the Article 29 Working Party advises that businesses should use 'prior opt in consent mechanisms' to obtain user consent.[190] Prior opt-in methods operate by the ISP giving users an opportunity to understand what cookies are and how they are being used before they are employed.[191] By using an opt-in method, organisations will also fulfil the obligations contained in Recital 66 of Directive 2009/22/EC.[192] This recital requires that users are provided with clear and comprehensive information before any data mining technology is used.

The United Kingdom implemented the *Cookie Directive (2009/136/EC)*[193] in its changes to Regulation 6(2b) of the *Privacy and Electronic Communications Regulations 2003* (UK).[194] Organisations in the United Kingdom are now required to provide comprehensive detail and obtain consent before using any data collection or storage technologies. In implementing these regulations, the Information Commissioner advises that 'setting cookies before users have had the opportunity to look at the information provided … is likely to lead to [regulatory] compliance

---

189 Information Commissioner's Office, above n 117, 6.

190 Article 29 Working Party set up under Article 29 of Directive 95/46/EC, *Opinion 15/2011 on the Definition of Consent* (adopted on 13 July 2011), 16 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf>.

191 Information Commissioner's Office, above n 117, 6.

192 *Directive 2002/22/EC of the European Parliament and of the Council 7 March 2002 on Universal Service and Users' Rights Relating to Electronic Communication Networks and Services* [2002] OJ L 108/55.

193 *Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and User's Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on the Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws* [2009] OJ L 337/11.

194 *Privacy and Electronic Communications (EC Directive) Regulations 2003* (UK) s 6(2b).

problems'.[195] To comply with this Act, organisations should tell people that cookies are there, explain what the cookies do and obtain their consent to store a cookie on their device.[196]

Despite this, 'prior opt-in' methods allow organisations to acquire implied consent after cookies have been used. This is evident from websites in the United Kingdom that advise the user that they will have accepted the use of cookies unless they manually change the privacy settings on their computer. By way of an example, a website has used a prior opt-in method with the following terms:

> [w]e use cookies to help make this website better. To find out more about the cookies we use, please read our Cookies Policy. If you continue without changing your cookie settings, you consent to this use, but if you want, you can find information in our Cookies Policy about how to remove cookies by changing your settings. [197]

One of the weaknesses that this creates is that cookies can be placed instantaneously onto the user's hard drive upon their arrival at the website. This creates a significant lapse in the degree of control that is provided to users.

This regulatory system has made a degree of progress in providing an adequate amount of privacy protection in the European Union. However, the system fails to grasp the instantaneous exchange occurring on the internet by allowing organisations to obtain implied consent. It becomes evident that due to the nature of the internet, only express consent should be allowed before any data mining technology is utilised. It is admitted that the European Union's directive regarding cookies could cause problems to online commerce. It could discourage new users from visiting websites that comply with the directive. Some online businesses may move jurisdictions so that they are not required to follow the directive. It is estimated that the directive could cause businesses to lose billions

[195] Information Commissioner's Office, above n 117, 6.
[196] Ibid 11.
[197] This particular example is extracted from the 2015 Rugby World Cup website.

of pounds.[198] The European Union directive is still positive, notwithstanding any resulting detriment.

V PROPOSED CHANGES TO AUSTRALIAN LEGISLATION

Studies have shown that industry self-regulation without governmental intervention fails to protect individuals' privacy.[199] The Australian Federal government should not rely on market forces to resolve the privacy concerns involved with cookies and should legislate on the issue. The first proposal is to expressly modify the *Privacy Act* to apply to data collecting techniques. Companies such as Facebook would then be required to expressly disclose any information that it gathers by cookies.

Australian legislators should pass provisions that are similar to the *E-Privacy Directive (2002/58/EC)*[200] and the *Cookie Directive (2009/136/EC).*[201] Specifically, the Australian government should follow the European government's approach to require organisations that use cookies to give users an opportunity to refuse

---

[198] Olivia Solon, 'Compliance with EU Cookie Law Could Cause the UK £10 Billion', *Wired* (online), 24 April 2012, <http://www.wired.co.uk/news/archive /2012-04 /24/eu-cookie-law-compliance-%C2%A310bn>.

[199] Lynn Chuang Kramer, 'Private Eyes Are Watching You: Consumer Online Privacy Protection—Lessons From Home and Abroad' (2002) 37 *Texas International Law Journal* 387, 417.

[200] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector* [2002] OJ L 201/37, recital 25, art 6.

[201] *Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and User's Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on the Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws* [2009] OJ L 337/11 art 5(3).

the use of technology. To achieve this, the *Privacy Act* should expand the definition of 'consent' to require an ISP to obtain the user's express, rather than implied, consent. Use of cookie technology would become conditional upon the user's well-informed acceptance. Further research in this area could involve drafting short paragraphs about giving consent to use the information that a cookie collects. Researchers could note whether or not participants give their consent. They can also ask the participants who refuse to provide their consent their reasons.

The changes to Australian legislation should also require that an ISP obtain consent through a click-wrap contract. Such contracts operate by requiring the user to click a button marked 'I Agree' or 'I Accept' and gives users the opportunity to read how the technology operates before it is used.[202] Under this system users could access all information about how cookie technology operates before it's used. The click-wrap contract would also prevent Facebook, and similar sites, from gathering information about users through using third-party cookies. The click-wrap contract would act to mitigate against the instantaneous nature of the internet and require organisations to obtain express consent before using data gathering technologies. An example of a click-wrap contract of this nature may take the following form:

> This website uses, and has in place from partner websites, cookies that gather personal information about you. If you agree to the use of cookies please click 'accept'. If you disagree to the use of cookies please click 'I do not accept'.
>
> If you would like further information on how this website uses cookies please click 'further information'.
>
> If at the end of your session on this website you wish to access your personal information, then you may do so by clicking the 'Access to Information' link located at the top right hand corner of this page.
>
> I Accept I do not Accept Further Information

[202] These are often used to create binding contracts on internet users for e-commerce transactions, see Clive Turner, *Australian Commercial Law* (Thomson Reuters, 28th ed, 2011) 295.

This sample click-wrap contract makes it explicitly clear to the user that the ISP is using cookie technology to gather personal information about them. The contract also provides a link for the user to gain further information about cookie technology. This will allow the user to access information on how the technology works and how data about them is stored. The click-wrap contract also directs users to where they can access any personal or sensitive information that was stored about them.

Under this click-wrap contract an ISP must obtain informed consent and also allow access to the information gathered by cookies. The consent under this contract creates an 'opt-in' system requiring express consent before the use of the data-mining technology. This will give internet users protection as soon as they visit a website and takes into account the instantaneous nature of the internet. The changes will also put the internet 'on notice' of any data gathering techniques that are taking place on the internet. Admittedly, it is possible that users may simply press 'I Accept' in the click-wrap contract and not read its first three paragraphs. It is to be hoped that the majority of users would read the entirety of the contract.

The proposed amendments to the *Privacy Act* will help to ensure that Australians are given the minimum level of privacy protection that the Control Theory of Privacy requires. This is because the system will make it compulsory for organisations to obtain express consent and to direct users to how to access their stored personal information. The protection will grant users overarching control of their personal information through the ability to amend or delete any data profile that has been created. Users will also be expressly put on notice about the existence of data gathering technology on the internet. Through this they will be able to monitor their personal data to ensure that any information about them is not inadvertently given to governmental agencies. This will also act to prevent data trading between security agencies, allowing individuals to protect their privacy. This click-wrap contract uses plain English, so it should be relatively easy for Australians to understand. It would be possible to make the click-wrap contract available in additional

languages so that users could choose to read the contract in those languages.

The access to stored data will relate to any client or consumer profile that has been created about them by the ISP. It will also be limited to profile-style websites where the gathered data can be easily correlated to a specific user (such as Facebook profiles). This will allow users access to the stored data on websites where they have created a specific user-profile.[203] Unlike the current system of access, the data must be presented in a simplistic, non-technical form. It must reveal to the users how that information is relevant to the organisation and how it has been used. Access must also be given to any client or consumer profiles that were created about the users from this information.[204]

The Australian government should implement legislation that regulates data mining technologies more effectively. The legislation should require all ISPs to obtain express consent from users before gathering personal or sensitive information. Websites that have a user account (such as Facebook) should allow individuals to access any stored data or client profile that was created about them.

VI CONCLUSION

This article argued that there's a need for privacy to develop individual thought. This need exists because if privacy is constantly infringed, then ideas, behaviour and attitudes will be modified as

[203] This can include a user's *Twitter*, *Amazon.com* or *Google* account.

[204] This particular part of the proposal may face constitutional challenges. This is because, as proposed in van Dijk, above n 26, the consumer profiles are created by unique and highly protected algorithms. By forcing companies to grant access to the information the Federal Government may be inadvertently 'acquiring' the intellectual property rights contained in these consumer profiles. The proposed legislative reform may then have some issues regarding section 51(xxxi) of the *Constitution* (the acquisition of property on just terms). Such an argument is an important consideration but is beyond the scope of this article.

people become aware that their movements are being watched. This leads to society creating self-enforced norms that endorse what are considered to be acceptable activities. The constant invasion of privacy then causes a decline in unique and individual thought that hinders societal development and innovation.

Facebook's use of cookie technology has been provided as an example of how modern technology has begun to infringe upon this fundamental right to privacy. Facebook has the ability to plant these cookies on an undisclosed number of partner websites. This data can be matched to an individual user's personal Facebook profile that already contains a great level of personal information. This includes information such as: a person's hometown, relationship status and 'checked-in' locations. Facebook can then take this data about its users to provide targeted advertisements from its affiliates. While the recent changes to the APPs provide some headway in dealing with target advertising, they do not directly deal with the issues of gathering and storing data (third-party cookies in particular). The focus of the legislation has been on how the information is used rather than how it is obtained. The need to regulate gathering information by cookies needs to be a focus because the issue extends beyond targeted advertisements and includes the prospect of personal information being used by domestic and international government agencies.

To protect privacy on the internet, users must be able to control any information that organisations wish to obtain. This view accords with the Control Theory of Privacy. This theory proposes that privacy is best protected when users have the ability to determine for themselves when, how, and to what extent information about them is communicated to others. In a way this attaches quasi-property rights to personal information that can be traded for the use of a service so long as there has been full disclosure about how tracking techniques are used.[205] This will allow users to be aware of cookies and how they can be used.

[205] As explained in van Dijk, above n 26, 58-59; Davidson and Bryant, above n 2, 10.

The current legal landscape in Australia allows too many large internet companies to gather excessive amounts of personal information. Any potential legal or equitable right to privacy will only provide protection to users when they have suffered actual 'harm'. This may include a circumstance where a celebrity makes the front page of a tabloid magazine after being photographed outside a narcotics anonymous centre.[206]

The legislative protection provided under the *Privacy Act* requires that ISPs only gain consent before collecting sensitive information. A critical flaw within the definition of consent is that it operates on an opt-out basis. Users are therefore often left ignorant about any data mining activity that is undertaken. Further, the *Privacy Act* does not require ISPs to allow users to access any consumer or client profile that is created about them. This gives individuals limited capacity to alter and amend any incorrect information stored about them.

More regulation is needed to fix this current predicament and grant Australians an adequate level of privacy protection. Simply leaving it to the market will not suffice. The regulation should demand an opt-in system requiring that express consent is obtained before any cookies are used. This consent should be acquired through the use of a click-wrap contract that allows users to obtain further information about cookies before they are used. The consent would therefore be fully informed. If the website contains a detailed personal account of the user, such as a Facebook profile, then the user must be able to access all information that is collected about them, including any client profile. This will give users control over the personal information and the ability to change any incorrect data to protect them from any unauthorised use.

Currently, Australian legislation is not keeping pace with developing technologies and further research is necessary in other

[206] Such as that which occurred in *Campbell v Mirror Group Newspapers Ltd* [2003] 1 All ER 224.

areas of privacy invasion.[207] It is envisaged that Australia will pass laws that require individuals to 'opt-in' when they face any information or data gathering practices. This will enable individuals to be fully aware of the extent that they are being tracked as well as the ability to control the level of information that they disclose.

Further research is necessary about whether granting access to consumers' or clients' profiles held by organisations would be acquiring their intellectual property rights. If this is the case, then the legislative initiatives proposed may be hindered by section 51(xxxi) of the *Constitution*.

It should now be evident that tracking by corporate entities occurs every day at nearly every moment. This vast level of data gathering is shaping the world to become an Orwellian fantasy, with the Zuckerberg Cookie Monster being but one Big Brother. The Australian government should implement opt-in regulation to stop the Zuckerberg Cookie Monster from continuing to satisfy its large appetite.

[207] See, eg, the discussion of Location Aware Technologies in Gilbert, above n 38. See also John Brandon, 'Retail Stores Plan Elaborate Ways to Track you', *Fox News* (online), 26 July 2013, <http://www.foxnews.com/tech/2013/07/26/retail-stores-plan-elaborate-ways-to-track/>; Jake Sturmer, 'Use of Phone-Tracking Technology in Shopping Centres Set to Increase', *ABC News* (online), 29 August 2013, <http://www.abc.net.au/news/2013-08-29/use-of-phone-tracking-tech-in-shopping-centres-set-to-increase/4923298>; Lucy Battersby, *Tracked From the Moment You Wake: Buyer Beware. Who we are and What we do is no Longer a Secret (*24 August 2013), <http://www.smh.com.au /technology/technology-news/tracked-from-the-moment-you-wake-20130824-2 shwq.html>; Dave Lee, 'New Adverts 'Could Track Your Eyes' in Supermarkets', *BBC News* (online), 30 April 2013, <http://www. bbc.co.uk/news/technology-22351995>; Ashley Lutz and Alaina McConnell, '12 Sneaky Ways That Big Retailers Track Your Every Move', *Business Insider* (online), 1 January 2013, <http://www.businessinsider.com/retail-tracking-2012-12?op=1/?IR=T>.