RESEARCH NOTE

PRODUCED FOR THE

QUEENSLAND COUNCIL FOR CIVIL LIBERTIES (QCCL)

BACKGROUND & LEGISLATIVE STATUS OF 'DO NOT TRACK' LEGAL INITIATIVES

Authored by:

Ms Brigette Garbin and Ms Kelly Staunton
under the supervision of Dr Mark Burdon

T. C. Beirne School of Law,
University of Queensland

EXECUTIVE SUMMARY

Online behavioural profiling is 'the practice of tracking an individual's online activities in order to deliver advertising tailored to the individual's interests'. It has now become an industry that is worth billions of dollars throughout the globe. The actual practice of tracking was once limited to individual websites and individual cookies. However, the development of new technologies has enabled marketing corporations to track the web browsing activities of individual users across the internet. These corporate activities raise a number of privacy concerns:

- Individual users are often unaware that their internet usage history is being collected and tracked. The issue of consent is therefore important.
- Individuals have little recourse to access data collected about their web browsing activities and challenge any inaccuracies.
- Online tracking companies have little transparency and are largely unaccountable in predominantly self-regulatory frameworks. Moreover, there appears to be almost no practical legal limits on what data can be collected and how it can be used.
- Despite assurances to the contrary, there exists growing concern that through the process of data collection and the creation of a 'profile' of an online user, their identity will be revealed.
- Recent activities by Google have also demonstrated that existing Do Not Track mechanisms can easily be circumvented.

Consequently, it should be no surprise that legislative initiatives are afoot. There is a significant amount of legislation before the US Congress dealing with online behavioural profiling. Currently the FTC is entitled to take action in order to protect consumer rights when a business engages in unfair or deceptive practices, or more specifically, where they do not adhere to their own privacy policies. The proposed legislation offers varying degrees of state involvement in the behavioural advertising industry, from simply the introduction of a mandatory mechanism to elect whether or not to be tracked, to the more

complex and encompassing privacy rights and obligations enumerated by the Obama administration in the White Paper. Both the White Paper and the Commercial Privacy Bill of Rights Act propose a "safe harbor" program by which companies could keep or design their own privacy policies, which would be approved and subsequently enforced by the FTC as an alternative to their adherence to legislation. Initiatives have also been undertaken in the EU and Canada.

It is currently unclear exactly what application the Australian Privacy Act will have regarding the collection of user browsing activity for the purpose of online behavioural profiling. The first issue to resolve is whether the information collected for the purpose of online behavioural profiling is personal information. Second, the applicability and coverage of National Privacy Principle 2 needs to be clarified in relation to Do Not Track mechanisms. Third, clarification is required about whether the secondary use of data profiling purposes meets the requirements of National Privacy Principle 2. Finally, the application of the small business exemption may have a debilitating effect on coverage under the Act.

The typology developed in this research note highlights that different jurisdictions have put forward different methods of regulating online behavioural profiling and Do Not Track initiatives. Three broad approaches are apparent:

- The predominantly self-regulatory approach adopted in Australia and currently in the US;
- The co-regulatory approach of Canada; and
- The prescriptive, legislative approach of the EU.

These three systems are not absolute, and no jurisdiction entirely uses one approach to the total exclusion of the other. They can rather be considered a spectrum with self-regulation dominating at one end, and state regulation dominating at the other. Australia has a largely self-regulated industry of targeted advertising. However, a predominantly self-regulatory approach for privacy protection tends to go hand-in-hand with a relatively weak legislative framework, as has been frequently argued about the US legal framework. This statement

could also be applied to Australia. An approach that is too far towards the self-regulated end of the spectrum arguably leaves consumers more vulnerable and dependent on the individual policies and practices of particular organisations.

Consequently, several recommendations were considered that would seek to strengthen the current Australian framework:

- Strengthening the existing self-regulatory framework by introducing elements of co-regulation found in Canada;
- In turn, this would require greater statutory powers for the Privacy Commissioner;
- Providing individuals with options that incorporate their meaningful consent;
- Reducing the scope of the small business exemption;
- Stronger regulation for transborder information flows particularly in relation to online behavioural profiling issues and
- Considering the development of a new statute specifically for online privacy.

The issues of online behavioural profiling and Do Not Track legal responses are garnering world-wide interest. How Australia will respond to these developments is as yet unclear. However, it would appear from global initiatives that there is a distinct move away from predominant self-regulatory approaches to more nuanced, legislative options. Given the global nature of online behavioural profiling, it is likely that Australia will have act in some form or another as maintaining the status quo for the sake of it may not be a viable option.

Contents

1 INTRODUCTION 6

2 BACKGROUND – HOW ONLINE BEHAVIOURAL PROFILING OPERATES 6

2.1 PRIVACY CONCERNS 8
2.2 CURRENT MECHANISMS FOR PREVENTING TRACKING 10
2.3 RECENT CONTROVERSIES 11

3 US LEGISLATIVE DEVELOPMENTS 13

3.1 THE DIGITAL ADVERTISING ALLIANCE 13
3.2 THE CONSUMER PRIVACY BILL OF RIGHTS 14
3.3 THE COMMERCIAL PRIVACY BILL OF RIGHTS ACT OF 2011 BILL 16
3.4 THE DO-NOT-TRACK ONLINE ACT OF 2011 BILL 17
3.5 THE DO NOT TRACK ME ONLINE ACT BILL, 2011 17
3.6 CALIFORNIA LEGISLATION – SENATE BILL NO. 761 18

4 OTHER JURISDICTIONAL DEVELOPMENTS 18

4.1 EUROPEAN UNION LAW 19
4.1.1 Data Protection Directive 1995 19
4.1.2 Article 29 Working Party 20
4.1.3 E-Privacy Directive 2002 20
4.1.4 General Data Protection Regulation 2012 21
4.1.5 EASA Best Practice Recommendations 22
4.2 NEW ZEALAND 23
4.3 CANADA 24

5 AUSTRALIAN DEVELOPMENTS 24

6 ANALYSIS & RECOMMENDATIONS 28

6.1 TYPOLOGY OF REGULATORY APPROACHES 29
6.2 RECOMMENDATIONS FOR AUSTRALIAN DO NOT TRACK INITIATIVES 33
6.2.1 Strengthening the Self-Regulatory Framework 33
6.2.2 Enhancing the Powers of the Privacy Commissioner 34
6.2.3 Providing Meaningful Consent 35
6.2.4 Reducing the Scope of the Small Business Exemption 37
6.2.5 Regulating Transborder Information Flows 37
6.2.6 Developing A New Online Privacy Statute? 38

7 CONCLUSION 39

1 INTRODUCTION

The Queensland Council for Civil Liberties wrote to Dr Peter Billings on 15 February 2012 to request that the T.C. Beirne Pro Bono Centre undertake research into legislation to protect internet privacy, particularly recent legislative proposals related to Do Not Track initiatives. Two students were chosen to undertake the research under the supervision of Dr Mark Burdon, who has a primary research interest in Privacy Law. Ms Brigette Garbin is a final year law student and Ms Kelly Staunton is currently in her penultimate year at the Law School.

This research note is intended as a background briefing to the complex issues that arise out of online behavioural profiling and subsequent Do Not Track proposals. Section 2 provides an overview of how online behavioural profiling operates, the privacy concerns that arise and highlights recent contemporary controversies. Section 3 details Do Not Track legislative initiatives that have recently taken place in the United States (US). Section 4 outlines developments in the EU, Canada and New Zealand and Section 5 overviews recent Australian developments. Section 6 provides a typology of Do Not Track regulatory approaches and concludes with suggested recommendations for legislative improvements based on the analysis of jurisdictional approaches and recent Australian developments.

2 BACKGROUND – HOW ONLINE BEHAVIOURAL PROFILING OPERATES

Online behavioural profiling is 'the practice of tracking an individual's online activities in order to deliver advertising tailored to the individual's interests'.[1] The actual practice of tracking was once limited to the installation of traditional cookies that record the websites a user visits.[2] However, marketing and advertising companies are now employing a range of new tools such as flash cookies, third-party cookies and beacons in order to track the online behaviour of individuals.[3] *Third party cookies* are the primary mechanism used for online tracking. These cookies are operated by a 'third party', the advertising or marketing

1 Federal Trade Commission, '*Self-regulatory principles for online behavioural advertising*', (2009) available from http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf at 12 April 2012.

2 See Wall Street Journal, '*A Short Guide to Cookies*' http://online.wsj.com/public/page/0_0_WP_3001.html?currentPlayingLocation=158&currentlyPlayingCollection=Tech&currentlyPlayingVideoId={92E525EB-9E4A-4399-817D-8C4E6EF68F93} at 12 April 2012, for a short video that provides an excellent overview of the history, development and use of cookies by marketing organisations.

3 EPIC, '*Online tracking and behavioural profiling*', http://epic.org/privacy/consumer/online_tracking_and_behavioral.html at 12 April 2012.

company, as opposed to the actual domain a web user is visiting, and place its cookies on the domain that a user is browsing. Generally speaking, third-party cookies will be placed by advertising network domains, allowing them to construct a 'profile' of an online based on their browsing activities that is subsequently used for the purpose of delivering targeted advertisements.[4] Online behavioural tracking has become a burgeoning industry precisely because of the potency of advertising that it provides for.[5] A user who chooses to remove cookies can still have their data accessed as a result of *flash cookies*, devices that re-install deleted cookies. *Beacons* are used by online tracking companies to track a user's every movement on a website, including what is typed and where the user is moving the mouse. The data that people are accessing or browsing on a webpage can be collected in real-time, and then be aggregated with other data about a particular user, including their location, income, hobbies and so on.

The aggregation can be primarily conducted in two ways depending on what information is being collected by the relevant cookie. First, by aggregating data around the Internet Protocol (IP) address of the device that is being used to access the web page. In this situation, it may or may not be possible to identify and aggregate information to an individual as data is being aggregated to a device (e.g. a computer or smart phone) rather than a person. However, it is potentially a relatively simple task to ascertain an identity from an IP address.[6]

Second, aggregation is also completed by aggregating data around a specific individual identifier. For example, Target (US) is able to aggregate data about an individual because it assigns a unique code – a Guest ID number – to all customers who transact or visit the Target website, which forms the basis for data aggregation.[7] Google operates in a similar

[4] See Duhig, C, 'How Companies Learn Your Secrets' available from http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=1 at 12 April 2012, for an excellent overview of how the US retailer, Target, collects and uses individual purchases and internet tracking data for advertising purposes. The targeting processes are so sophisticated that the company can identify specific groups of individuals, such as pregnant women, which are then targeted with adverts for specific baby related products.
5 Phillips, N, '*Inside the cookie monster - trading your online data for profits*' The Australian (5 October 2010).
[6] See for example, IPGP, *IP Address Lookup,* http://www.ipgp.net/ at 12 April 2012, as an example of online services that provide locations for IP addresses.
[7] Duhig, above n. 5.

fashion in relation to any web user that has a Google account and is logged in to that account.[8]

2.1 PRIVACY CONCERNS

There are several privacy concerns linked to tracking and the collection of data for the purposes of online behavioural profiling. Individual users are often unaware that their internet usage history is being collected and tracked. The issue of consent is therefore important and is often raised by groups opposed to online tracking. They argue that the information collected online is not information that consumers voluntarily consent to being shared with tracking companies and online advertising businesses.[9] Public sentiment would seem to support this argument, with a US Gallup poll revealing that 67% of internet users do not believe advertisers should be allowed to match ads to your specific interests based on websites you have visited.[10] Similarly, a recent Australian survey undertaken by the Centre for Critical and Cultural Studies, the University of Queensland found that only 36% of 965 respondents were comfortable with tailored advertising as a concept. Of these, 39% were uncomfortable with the idea that their information would be shared across websites.[11]

Furthermore, users are potentially at a distinct disadvantage as they may be unable to easily access internet browsing information collected about them, or correct any inaccuracies, leading to a concern that online tracking companies have little transparency and are consequently unaccountable.[12]

A further danger arises from the development of 'digital dossiers' of aggregated data which are used by corporations and governments to make decisions that direct affect individual livelihoods. These dossiers are used as if the information collected *is* the person when in reality the aggregated data merely provides a potentially inaccurate snapshot of an

[8] As clarified by Google's new privacy policy. See Google, Privacy Policy http://www.google.com/policies/privacy/ at 12 April 2012.
9 EPIC, above n. 3.
[10] Gallup, 'US Internet Users Ready to Limit Online Tracking for Ads' available from http://www.gallup.com/poll/145337/internet-users-ready-limit-onlinetracking-ads.aspx
[11] Andrejevic, M and Arnott, C, 'Internet Privacy Research', (2011) available from http://cccs.uq.edu.au/documents/privacy-report.pdf
12 EPIC, above n. 3.

individual's online life.[13] Yet these dossiers can be used in real life for inclusion in marketing and advertising streams based on the perceived socio-economic status of certain communities of individuals. However, with inclusion also comes exclusion, which can lead to the development of segregated communities in which those individuals and families with less economically attractive digital dossiers are effectively excluded from access to certain marketing information.[14]

The type of information collected is also another troubling aspect of online tracking. Because the industry is largely self-regulated, there appears to be almost no practical legal limits on what data can be collected and how it can be used.[15] Perhaps a more extreme example of this is the ability of advertisers to track people with health problems such as bipolar disorder, through the tracking company Healthline.[16] This then allows advertisers to target these people with ads related to bipolar disorder or other sensitive medial ailments on the assumption that an individual is content for such knowledge to be disclosed or attributed.[17]

Finally, there exists growing concern that through the process of data collection and the creation of a 'profile' of an online user, their identity will be revealed. It is argued by marketers that online browsing data is anonymous because it identifies web browser related statistics rather than individuals.[18] However a Wall Street Journal researcher has explained that the aggregation or collection of 33 'bits' of information about a particular user will be enough to expose their identity and de-anonymise the data collected.[19] When it is taken into account that certain websites transmit roughly 26 'bits' of information about a user, it becomes clear that these privacy concerns are not without merit.[20] This point is further encapsulated by mass data aggregation processes such as those figured around the use of third party cookies or beacons.

---

[13] Daniel J. Solove, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy' (2001) 53(6) *Stanford Law Review* 1393

[14] See Turow, J, 'The Daily You' (2011), 2-4 for an example of social exclusion through social sorting.

15 Phillips, above n. 5.

[16] Healthline, http://www.healthline.com/ at 12 April 2012.

17 EPIC, above n. 3.

18 Phillips, above n. 5. See also Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' 57 *UCLA Law Review* (2010) regarding the inherent difficulties of truly anonymising personal data.

19 Narayanan, A, 'Do Not Track Explained - 33 bits of entropy', September 20, 2010, http://33bits.org/2010/09/20/do-not-track-explained/ at 12 April 2012.

20 Ibid.

2.2 CURRENT MECHANISMS FOR PREVENTING TRACKING

The Consumer Federation of America and Consumers Union argues that "there is a fundamental mismatch between the technologies of tracking and targeting and consumers' ability to exercise informed judgment and control over their personal data."[21] A study by Carnegie Mellon University also criticises the current internet privacy tools designed to protect consumers from online behavioural profiling, labelling them hard for the average user to understand and configure.[22] The study tested several tools, including tools that block access to advertising websites, tools that set cookies indicating a user's preference to opt out of online behavioural profiling, and privacy tools that are in-built into web browsers.[23] Among the problems reported by study participants and researchers were:

- Communication issues in terms of the user being notified of the purpose of a tool and the way in which to configure it;
- Lack of feedback which would allow a user to be aware of whether or not the opt-out was working) and
- A tendency of some tools to cause websites to stop working or operate with limited functionality.[24]

As a result of these findings, the report concluded that the self-regulated status quo of online behavioural profiling is fundamentally flawed and insufficient for empowering users to protect their privacy online. Similarly, in 2010, the Federal Trade Commission (FTC) released a report which stated, among other things, that

"industry efforts to address privacy through self-regulation have been too slow...and have failed to provide adequate and meaningful protection."[25]

21 Consumer Federation of America and Consumers' Union, 'Comments to the FTC concerning the proposed online behavioural advertising self-regulatory principles' (April 11, 2008)
22 Cranor, L, et al, '*Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioural Advertising*', Carnegie Mellon University, (October 2011) [2] www.cylab.cmu.edu/research/techreports/2011/tr_cylab11017.html at 12 April 2012.
23 Ibid, [1]
24 ibid, [4]
25 Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, (2010) http://online.wsj.com/public/resources/documents/PrivacyReport_FINAL.pdf at 12 April 2012.

In response to these perceived failings, Do Not Track legal initiatives have been proposed to further regulate online behavioural profiling. One suggested model involves enabling users to configure their web browsers to send a Do Not Track header with HTTP requests, signalling that they do not want to be tracked.[26] Most recently, the US legislature has announced a framework for new privacy regulations, which would include a Consumer Privacy Bill of Rights whereby a set of enforceable practices would be negotiated with industry, consumer protection and privacy advocates. A 'Do Not Track' agreement, recently signed by a group of advertising networks and leading internet companies such as Google and Yahoo, is a first step towards this new model, and will lead to the adoption of DNT features integrated into web browsers. The FTC will be responsible for oversight and enforcement of the agreement's terms.[27] These developments are covered in greater depth in the next section.

2.3 RECENT CONTROVERSIES

During 2012, Google has been implicated in several Do Not Track controversies. On February 17, the Wall Street Journal revealed that Google had intentionally circumvented the privacy settings of Apple's web browser, Safari, for the purpose of setting its third-party advertising cookies.[28] Safari automatically prevents installation of cookies from ad networks and other third parties. However Google worked around this by exploiting a loophole in Safari that allows cookies to be placed when a user interacts with a website in some way, for example by filling out a form. Google added Javascript coding to some of its ads that caused Safari to think that invisible forms were being submitted to Google, thus paving the way for Google to install a temporary cookie on a phone or computer.[29] Upon testing the 100 most-visited US websites for the cookies placed by Google's display ad network on a Safari web browser, the Journal discovered that 22 of the websites installed

[26] Cranor et al, above n. 22, 6.

27 White House, '*White House announces new privacy 'Bill of Rights', Do Not Track Agreement*', http://arstechnica.com/tech-policy/news/2012/02/white-house-announces-new-privacy-bill-of-rightsdo-not-track-agreement.ars at 12 April 2012.

28 Angwin, J, '*Google's iPhone tracking*', Wall Street Journal, available at online.wsj.com/article_email/SB10001424052970204880404577225380456599176-%0A%0AlMyQjAxMTAyMDEwNjExNDYyWj.html?mod=wsj_share_email#articleTabs%3Darticle%26project%3DSAFARITRACKINGCODE0212 at 12 April 2012.

29 EPIC, '*Google's Circumvention of Browser Privacy Settings*', available at http://epic.org/privacy/google/tracking/googles_circumvention_of_brows.html at 12 April 2012.

the Google tracking code.[30] A day later, it was also revealed that Google had bypassed the cookie settings of Internet Explorer users by piggybacking on a 'nuance' with P3P specifications.[31]

Google's actions highlight how easily privacy settings in browsers can be bypassed, and this perhaps lends weight to the argument that legal reform, as well as technological reform, is necessary to ensure that online privacy standards are both difficult to circumvent and legally enforceable.[32]

Prior to the Safari and Internet Explorer revelations, Google had already been facing intense scrutiny and questions over its privacy practices. In January 2012, Google announced that from March 1 2012, it would consolidate its data from across its services (which include Gmail, Google+ and YouTube to name a few) to create a single merged profile for each user.[33] The policy change was marketed as a way for Google to provide a more complete, transparent and integrated service experience for users. However, it was met with considerable international opposition, particularly from the EU, whose privacy officials asked Google to 'pause' its changes until it could ensure the privacy of EU citizens.[34] Several EU data protection agencies have reached the conclusion that the policy violates the European Data Protection Directive in several ways. It was contended that Google's new privacy policy because it:

- Was not in accordance with the EU law regarding data transparency;
- Utilised the data of individuals in order to hand it over to third parties; and
- Provided inadequate notification and consultation prior to the implementation of the policy.[35]

30 Angwin, above n. 28.
31 Musil, S '*Microsoft: Google Bypassed IE Privacy Settings Too'* http://news.cnet.com/8301-1009_3-57381371-83/microsoft-google-bypassed-ie-privacy-settings-too/ at 12 April 2012.
32 Brodkin, J, '*Web privacy standards: easy to break, hard to enforce'*, http://arstechnica.com/tech-policy/news/2012/02/web-privacy-standards-easy-to-break-hard-toenforce.ars at 12 April 2012.
33 EPIC, 'above n. 29. ,
34 Angwin, above n. 28
35 Brodkin, J, '*Google privacy change taking effect today is illegal, EU officials say'*, http://arstechnica.com/tech-policy/news/2012/03/google-privacy-change-taking-effect-today-is-illegal-eu-officials-sayers at 12 April 2012.

The Electronic Privacy Information Centre (EPIC) has also been vocal in its opposition, and has filed a lawsuit against the FTC on the grounds that Google's new policy violates a consent order the company signed with the Commission in March 2011 after the Google Buzz controversy (which allegedly bars Google from opting users into services). Google, however, believes that it will withstand the legal challenge because the FTC consent order relates to the company's sharing of information with third parties, which the new privacy policy will not affect.[36] In response to EU objections, Google is similarly confident that the policy 'respects all European data protection laws and principles'[37].

3 US LEGISLATIVE DEVELOPMENTS

A number of Do Not Track initiatives have commenced in parallel across the US in recent years. These initiatives include the self-regulatory regimes of the Digital Advertising Alliance (DAA); the Obama Administration's Consumer Privacy Bill of Rights; federal legislation introduced in both the House and the Senate; and California state legislation. While self-regulation has tended to dominate as the preferred approach to online privacy, new legislation would introduce stricter rules and harsher penalties for companies failing to comply with industry codes of conduct. These codes would be enforceable by the FTC, state attorney generals, and in some cases by citizens as a private right of action.

3.1 THE DIGITAL ADVERTISING ALLIANCE

The DAA consists of a number of different advertising and marketing companies and groups, including the America Association of Advertising Agencies, the Association of National Advertisers, the Council of Better Business Bureaus the Direct Marketing Association and the Interactive Advertising Bureau. The regulations prescribed by the DAA are largely based on self-regulation, but the DAA uses monitoring programs and public complaints to oversee breaches of the regulations, which may be reported to government agencies if not remedied.[38]

36 Johnston, C, '*Google's new privacy policy could anger FTC*', http://arstechnica.com/gadgets/news/2012/01/pascals-wager-googles-new-privacy-policy-could-anger-ft.cars at 12 April 2012.
37 Brodkin, above n. 35.
38 American Association of Advertising Agencies, *'Digital Advertising Alliance Begins Enforcing Next Phase of Self-Regulatory Program for Online Behavioural Advertising'*, http://www.aaaa.org/news/press/Pages/052311_digital_next.aspx at 12 April 2012.

The DAA has released two sets of self-regulatory principles governing online tracking. The first set of principles, released in 2009, was the *Self-Regulatory Principles for Online Behavioural Advertising*. This included measures such as educating consumers, transparency in privacy notices, website-based consumer control over whether third parties or internet service providers (ISPs) monitor their activity, data security and accountability safeguards and prohibitions against collecting sensitive data – that is, data related to children under 13 or information related to health or finances.[39] While this document originally endorsed website-based consumer controls, facilitating site-by-site opt-outs of online tracking, in February 2012 the DAA announced that they were beginning work to bring into force a browser-based mechanism with the same purpose.[40]

Supplementing the *Self-Regulatory Principles* was the 2011 release of the *Self-Regulatory Principles for Multi-Site Data*. This document applies principally to ISPs and third-party data monitors. It adopts self-regulatory principles which attempts to prohibit the use of multi-site data without permission from the consumer, except for the purpose of operating the business, for market research or when the data will be de-identified within a "reasonable" time.[41] It absolutely prohibits the use of multi-site data to determine eligibility for employment, credit, insurance or health care treatment. Furthermore, it bans third parties or ISPs from collecting sensitive information, such as data related to the activity of children online, social security or financial information, or medical records.[42]

3.2 THE CONSUMER PRIVACY BILL OF RIGHTS

The Consumer Privacy Bill of Rights was proposed by the Obama Administration in February 2012, as part of the larger policy paper *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in a Networked World* (The White Paper).[43] The paper expounds a Consumer Privacy Bill of Rights, calls for

39 Digital Advertising Alliance, '*Self-Regulatory Principles for Online Behavioural Advertising*', 9-17 http://www.iab.net/public_policy/behavioral-advertisingprinciples at 12 April 2012

40 Digital Advertising Alliance, '*White House, DOC and FTC Commend DAA's Self-Regulatory Program to Protect Consumer Online Privacy: DAA Announces Plans to Expand Program Consumer Choice Mechanisms*' (Press Release, 23 February, 2012) http://www.aaf.org/default.asp?id=1322 at 12 April 2012.

41 Digital Advertising Alliance, '*Self-Regulatory Principles for Multi-Site Data*, 3 http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf at 12 April 2012.

42 Ibid., 4-6.

43 White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in a Networked World* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf at 12 April 2012.

consultation with commercial stakeholders to develop an enforceable code of conduct and establishes a Safe Harbor program for businesses. Notably the report does not call for a browser-based Do Not Track mechanism, although it endorses the efforts of private groups to develop such a mechanism.[44]

The Consumer Privacy Bill of Rights forms the main part of the report, and includes as its centre seven consumer rights:

- ***Individual Control:*** Companies (including search engines and third-party data brokers) should request permission from users to collect their information at the time that data collection begins. Consumers have the right to refuse tracking and recording of their data.

- ***Transparency:*** Privacy policies should be prominently displayed on a website and easy to read and understand. Emphasis should be given to terms which allow a website to collect information in excess of what is necessary for the given transaction.

- ***Respect for Context:*** Companies must disclose the purpose of data collection at the time of collection, and only use the data for the disclosed purpose. If companies wish to reuse the data for a different purpose, they may only do so if they seek permission from the consumer first ("individual choice") and are clear about what they will be reusing the data for ("appropriate transparency").

- ***Security:*** Companies must assess the level of security that is appropriate to protect the kind of data they collect. This is a matter of discretion for the company, but some protection will always be necessary.

- ***Access and Accuracy:*** Commercial companies and websites should allow consumers to correct their own personal information online. The process of correction should not raise additional security concerns.

44 Ibid., 12-13.

- ***Focused Collection:*** Companies should only collect the kind and amount of personal information that they need to deliver their services or accomplish their purposes. Once personal data is no longer required, it should be disposed of or de-identified securely.

- ***Accountability:*** Companies that collect personal data should ensure that their employees and subsidiaries handle this data securely and in accordance with the Privacy Bill of Rights. These companies also have an obligation to ensure that any third party given access to the data also uses it securely and appropriately.

The report also calls for multi-stakeholder processes to develop their own codes of conduct tailored to specific industries. These codes of conduct would be enforceable and reviewable by the FTC. If approved by the FTC, companies with their own codes of conduct would be given 'safe harbor' from the provisions of any future statutory Consumer Bill of Rights, and would only be held liable to their own codes of conduct. [45]

3.3 THE COMMERCIAL PRIVACY BILL OF RIGHTS ACT OF 2011 BILL

Senators Kerry and McCain introduced the Commercial Privacy Bill of Rights bill to congress in 2011. Like the Consumer Privacy Bill of Rights, this bill aims to protect consumer interests by ensuring that collected data and personally identifiable information is protected and disposed of appropriately; that consumers are given clear information and a choice as to whether they are tracked online; and that only information necessary for carrying out business is collected online.[46]

Like the Consumer Privacy Bill of Rights, this bill does not require a browser-based Do Not Track mechanism. It instead requires each individual website to alert consumers to their privacy policy before asking permission to track their activity. However, the general opt-out provision is supplemented by a provision whereby consumer must actively opt in to the collection of "sensitive personally identifiable information."[47] This includes information such as medical records, religious information, or data likely to cause economic or physical harm if released.

45 Ibid., 23-27, 37.
46 Commercial Privacy Bill of Rights Act of 2011, S.799, 112th Cong., 1st Sess. (2011), s 201-303.
47 Ibid., s 202(a)(3)(A)

The Commercial Privacy Bill of Rights Act does not create a private cause of action enforceable by citizens. The regulations prescribed by the bill must be enforced only by the FTC or the Attorney General of a state.

3.4 THE DO-NOT-TRACK ONLINE ACT OF 2011 BILL

In 2011, Senator Rockefeller introduced the Do-Not-Track Online Act of 2011 bill. The main purpose of this bill was to implement a "mechanism by which an individual can simply and easily indicate whether the individual prefers to have personal information collected by providers of online services."[48]

The FTC would be given power to implement the mechanism and enforce observance of the choices made by consumers. If a consumer were to use the mechanism to opt out of having their personal information collected, only necessary, anonymous or de-identified data could be collected.[49] Both the FTC and state attorney generals would be given the power to bring a civil action against companies that did not adhere to the obligations. However, this bill would not give rise to a private right of action.

Unlike many of the other bills concerning online tracking, this bill does not provide any guidelines regarding the safe storage, collection or use of data that the consumer has given companies permission to record.

3.5 THE DO NOT TRACK ME ONLINE ACT BILL, 2011

In February 2011, Representative Speier introduced the Do Not Track Me Online Act bill to the House. This bill calls for the FTC to "promulgate regulations…that establish standards for the required use of an online opt-out mechanism to allow a consumer to effectively and easily prohibit the collection or use of any covered information and to require a covered entity to respect the choice of such consumer to opt-out of such collection or use."[50]

The Bill incorporates many of the principles of the Privacy Bill of Rights, requiring companies to notify consumers when their data is being collected, and to respect the decision by consumers to forego tracking and targeted advertising. It also requires that

48 Do-Not-Track Online Act of 2011, S.913, 112th Cong., 1st Sess. (2011), s 2(a)(1).
49 Ibid., s 2(b)(1)
50 Do Not Track Me Online Act, H.R.654, 112th Cong., 1st Sess. (2011), s 3(a)

privacy policies and data collection policies are transparent and easily accessible; that consumers have access to the personal information collected about them (although there is no mechanism legislated to allow them to correct it); and that only the kind of data a consumer would reasonably expect to be collected in the course of their relationship with a website should be gathered.[51]

The bill enables the FTC to prescribe regulations governing the specific uses of personal data, and also empowers it to audit companies and enforce the provisions of the bill. It creates a civil cause of action for which the Attorney General or agents of a state can prosecute.[52]

3.6 California Legislation – Senate Bill No. 761

On February 18, 2011 Senator Lowenthal introduced Senate Bill 761, to add a section to the California Business and Professions Code. This addition is closely based on Speier's Do Not Track Me Online Bill, containing many of the same principles related to data protection, use and collection.[53]

However, this bill does not call for any sort of broad Do Not Track mechanism, recommending instead that individual websites provide a method for consumers to opt out of data collection and use. This bill also gives rise to a private civil cause of action, allowing citizens to press charges against companies that breach prescribed regulations for damages up to $1000.[54] Finally, it absolutely prohibits the sale, sharing or transfer of personal data, unless that is the nature of a commercial transaction undertaken.[55]

4 Other Jurisdictional Developments

Section 4 overviews Do Not Track developments in the European Union (EU), New Zealand and Canada.

51 Ibid., s 3.
52 Ibid., s 4, 5.
53 An act to add Section 22947.45 to the Business and Professions Code, relating to business. S.B.761. State of California. 18 Feb. 2011, s 22947.45(b)(2)
54 Ibid., s 22947.45(d)
55 Ibid., s 22947.45(c)

4.1 EUROPEAN UNION LAW

EU law has generally favoured an opt-in approach to online tracking and behavioural profiling. This represents a markedly different approach than that taken in proposed US legislation, and has led EU authorities to reject the self-regulatory regimes of the online behavioural profiling industry. The foundations of European online privacy law are currently found in the Data Protection Directive of 1995 and the E-Privacy Directive of 2002. However, in early 2012 the European Union released a new proposal for a privacy framework known as the General Data Protection Regulation, encompassing the principles of previous directives, as well as some new rights and obligations.

4.1.1 DATA PROTECTION DIRECTIVE 1995

The Data Protection Directive was introduced in 1995 and deals broadly with the processing of personal data and consumer privacy rights.[56] It requires that any "processing"[57] of personal data be specifically consented to, unless that processing is necessary to perform a contract between the person and the company collecting data, the processing is in the public interest, or it is a legal requirement.[58] It calls for personal data to be collected only for "specified, explicit and legitimate purposes"[59] and absolutely prohibits the processing or collection of data regarding race, politics, religion, trade unions, health or sexuality.[60]

The Directive further outlines several rights for consumers in relation to information collected about them. These include the right to:

- Be told who has access to their data and for what purpose;
- Access and edit incorrect information;
- The erasure of data that has already been processed; and

[56] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data, and on the free movement of such data* [1995] OJ L 281/31.
[57] Defined in Art 2(b) as *any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction*. This definition applies to the same term in all EU directives.
[58] Ibid., Art 7.
[59] Ibid., Art 6(1)(b).
[60] Ibid., Art 8(1).

- Object to the collection or sharing of information about them.[61]

It also requires data processing companies to notify government authorities and data subjects of when and how their information will be processed, and to carry out this processing securely and confidentially.[62] Finally, it prohibits data processors from sharing personal data with third-party countries not subject to the directive, unless that country is found to have "adequate" protections in place, or the consumer has given informed consent to have their information shared.[63]

4.1.2 ARTICLE 29 WORKING PARTY

Article 29 of the Data Protection Directive creates a Working Party, whose purpose is to deliver rulings on the adequacy of privacy protections developed by private advertising groups.[64] In December of 2011, the Working Party declared that under EU law there is a presumption that people do not wish to have their data collected or processed.[65] It therefore requires that users actively opt in to any collection or processing of their information, including the placement or use of cookies on a consumer's computer.

4.1.3 E-PRIVACY DIRECTIVE 2002

The E-Privacy Directive was introduced in 2002 to supplement the provisions of the Data Protection Directive in relation to providers of publicly available electronic communications services.

The E-Privacy therefore differs to the Data Protection Directive in that it does not apply universally but only applies to the telecommunications sector. The E-Privacy directive nonetheless gives more attention to technologies developed or propagated since 1995, such as cookies and spam. Cookies are considered in article 5(3) of the Directive.[66] As it was originally passed, this section simply required companies placing cookies to inform the user of the purpose of any data processing and give them the "right to refuse". This section

[61] Ibid., Art 10(a)(b), Art 14.
[62] Ibid., Art 16-17.
[63] Ibid., Ch IV.
[64] Ibid., Art 29.
[65] *Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising Adopted on 8 December 2011*, [2011] 02005/11/EN WP188, 6.
[66] *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 (Directive on Privacy and Electronic Communications)* [2002] OJ L 201/37, Art 5(3).

was amended in 2009 to only allow the placement of cookies "on condition that the subscriber or user concerned has given his or her consent."[67] The standard was therefore raised in 2009 to require explicit and specific opt-in consent to the placement of cookies and the collection of consumer information.

Article 6 of the Directive requires that data which has been processed by a publicly available electronic communications service provider and is therefore no longer needed must be de-identified and erased, unless it needs to be retained for billing purposes.[68] It may also be retained for direct marketing purposes or to provide value-added services; however, this use must be consented to by the user and this consent must be capable of being withdrawn at any time.[69]

4.1.4 GENERAL DATA PROTECTION REGULATION 2012

The General Data Protection Legislation proposed in January 2012 is a clarification of the general rules provided under the Data Protection and E-Privacy Directives.[70] However, the proposal is for a set of Regulations, rather than a Directive, making its provisions directly binding on all the countries of the European Union, without the need to transpose them into national law. The rights conveyed on consumers and the obligations of data processors are largely unchanged, with a few exceptions. Under the Regulations, consent must still be explicitly given for any data processing[71] and consumers have a right to know who has access to their data and what kind of processing it will undergo.[72] Similarly, the Article 29 Working Party of the Data Protection Directive is replaced under Article 64 of the Regulations by a newly founded, European Data Protection Board.

However, the General Data Protection Regulation also provides for a number of new situations and definitions. These include:

---

[67] *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 users' 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 cooperation between national authorities responsible for the enforcement of consumer protection laws* [2009] OJ L 337/11, Art 2(5)(3).
[68] Ibid., Art 6(1)(2).
[69] Ibid., Art 6(3).
[70] *Proposal for a Commission Regulation (EC) No 0011/2012 of 25 January 2012 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* [2012] COM(2012) 11 final.
[71] Ibid., Art 6(1)(a),
[72] Ibid., Art 15.

- A "right to be forgotten" when there are no legitimate reasons for a company to retain personal data and a person no longer wants their data to be processed;[73]
- An obligation on data controllers to provide "transparent and easily accessible" information to consumers about their data collection policies;[74] and
- An obligation for data processors to maintain documentation of all the processing operations they are responsible for.[75]

This regulation in the currently under discussion by the EU and is expected to take effect by 2015.

4.1.5 EASA BEST PRACTICE RECOMMENDATIONS

In April 2011 the European Advertising Standards Alliance (EASA) released its Best Practice Recommendations (BPR), a set of non-binding, self-regulatory principles intended to guide companies engaged in online behavioural profiling.[76] This guide contains many of the same principles as the EU directives and regulations, including notice, informed consent, and special regulations for sensitive information.

It recommends specifically the implementation of a mechanism that allows a user to give informed consent to third-party tracking by linking them to a User Choice Site. This site would enumerate the privacy policy and data collection practices of third party advertising companies.[77] However, this method of informing the consumer and seeking consent has been rejected by the Article 29 Working Party as inconsistent with European law.

In a 2011 decision, the Article 29 Working Party held that the opt-out scheme proposed by EASA did not satisfy current EU legislation.[78] They declared that European Directives require opt-in consent, prohibiting any website or company from collecting data before informed consent is given. The method proposed by EASA would most likely result in the

[73] Ibid., Art 17.
[74] Ibid., Art 11.
[75] Ibid., Art 28.
[76] EASA, *Best Practice Recommendation on Online Behavioural Advertising*, (2011) http://www.easa-alliance.org/page.aspx/386 at 12 April 2012.
[77] Ibid., 12-13
[78] *Opinion 16/2011 on EASA/IAB*, 6.

processing of some information before the user was able to opt out of the collection, and as such did not provide sufficient protection of consumer's online privacy rights.

4.2 NEW ZEALAND

The New Zealand privacy framework is regulated by the Privacy Act 1993. It operates in a similar fashion to the Australian legislation, containing privacy 'principles' rather than prescriptive rules. From 2008-2011, the New Zealand Law Commission (NZLC) conducted a four stage review of New Zealand Privacy Law. Stage Four, released on 2 August 2011, represented the culmination of the process and reviewed the Privacy Act 1993 with a view to updating and amending it. The key changes recommended by the NZLC included expanding the powers of the Privacy Commissioner, introducing mandatory data breach notification laws and clarifying the privacy requirements for cross-border outsourcing.[79] It was also put forward that the Privacy Commissioner ought to have the power to issue compliance notices to organisations (rather than merely responding to complaints) and conduct privacy audits of organisations when necessary.[80]

Finally, it was recommended that organisations that outsource personal information to another agency or organisation for processing or storage remain fully accountable for the storage, use and disclosure of that personal information. Furthermore, where a New Zealand agency or organisation discloses personal information to an overseas entity, the disclosing agency or organisation will be required to take 'reasonable steps' to ensure that the information disclosed will be 'subject to acceptable privacy standards'.[81]

Interestingly, the Commission did not recommend any changes to the Privacy Act to accommodate direct marketing and online behavioural profiling.[82] The Commission's report and recommendations are currently awaiting government response.[83]

---

[79] NZLC R123, 'Key Recommendations', *Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4*, http://www.lawcom.govt.nz/sites/default/files/publications/2011/08/key_recommendations_-_for_report_release.pdf at 12 April 2012.
[80] Ibid, 1
[81] Ibid, 3
[82] Ibid, 4
[83] See NZLC, *Review of Privacy*, http://www.lawcom.govt.nz/project/review-privacy?quicktabs_23=report at 12 April 2012.

4.3 CANADA

Canada has two federal privacy laws - the Privacy Act, which took effect in 1983, and the Personal Information Protection and Electronic Documents Act ('PIPEDA') of 2000. The Privacy Act applies to the personal information handling practices of federal government departments and agencies. PIPEDA sets out the ground rules for how private sector organisations may collect, use or disclose personal information in the course of commercial activities. Under the law, individuals are granted rights to access and request correction of the personal information collected by companies about them.[84]

PIPEDA provides that the knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.[85] It also stipulates that personal information should only be kept 'as long as it is needed'[86]. With regards to what is considered 'personal information' for the purposes of PIPEDA, a contextual approach is generally adopted and it is worth noting a 2003 finding in which it was concluded that the information stored by temporary and permanent cookies was deemed to be personal information.[87] Where an IP address can be associated to an identifiable individual, this is also considered personal information.[88] In a 2011 report, the Office of the Privacy Commissioner considered whether PIPEDA needed to be updated to respond to challenges faced by online tracking, profiling and targeting.[89] However other than suggesting changes to what is considered valid consent under the Act, the Report made only general observations and proposed to consider amendments at the upcoming second mandatory 5-year review of PIPEDA.

5 AUSTRALIAN DEVELOPMENTS

Australia's privacy framework is primarily governed at the federal level by the Privacy Act 1988 (Cth) (hereafter "*Privacy Act*"). The Act contains a set of Information Privacy

[84] See Office of the Privacy Commissioner of Canada, *Privacy Legislation in Canada* http://www.priv.gc.ca/fs-fi/02_05_d_15_e.cfm at 12 April 2012.
[85] Office of the Privacy Commissioner of Canada, *Report on the 2010 office of the Privacy Commissioner of Canada's Consultations on online tracking, profiling and targeting, and cloud computing*, http://www.priv.gc.ca/resource/consultations/report_201105_e.pdf, at 12 April 2012.
[86] Ibid
[87] Ibid, 23
[88] Ibid
[89] Ibid

Principles (IPPs) for public sector agencies and a set of National Privacy Principles (NPPs) for private sector organisations. The collection, use, disclosure, storage and destruction of personal information are dealt with under these privacy principles. The Office of the Privacy Commissioner (OPC) (now the Office of the Australian Information Commissioner [OAIC]) was also established by the *Privacy Act*.

In 2008, the Australian Law Reform Commission (ALRC) released a significant review of privacy law and practice[90], to which the Australian government announced a two-stage response. The first stage was released in October 2009, in the form of an exposure draft of amendments to the *Privacy Act* which was considered by the Senate Finance and Public Administration Legislation Committee.[91] The key purpose of the exposure draft was to replace the NPPs and IPPs with uniform principles, termed Australian Privacy Principles (APPs), applicable to both the public and private sector. The Senate Environment and Communications Reference Committee also released a report recommending Privacy Act amendments in 2011, entitled 'The adequacy of protections for the privacy of Australians online'. As of April 2012, the changes proposed in both the government's response and the Committee's report has not been implemented into the *Privacy Act*.

In response to the privacy concerns posed by online behavioural profiling, the Committee recommended that the OAIC in consultation with web browser developers, internet service providers and the advertising industry should develop a code which includes a 'Do Not Track' model following consultation with stakeholders.[92] In this respect, it expressed a preference to a model similar to that which the Federal Trade Commission proposed to the US advertising industry.[93] However, no action has thus far been taken by the OAIC on this point.

As regards the current application of the *Privacy Act* to online behavioural profiling, the Act may apply but even if it does, the coverage of application may not be universal to all websites.

---

[90] ALRC, *For Your Information: Australian Privacy Law and Practice,* Report No 108, 2008, www.alrc.gov.au/publications/report-108 at 12 April 2012.
[91] Senate Finance and Public Administration Legislation Committee, *Inquiry into Exposure Drafts of Australian Privacy Amendment*, 2010.
[92] Ibid, 44.
[93] Ibid.

The first issue to resolve is whether the information collected for the purpose of online behavioural profiling is personal information. Under s 6(1) of the Act, personal information is information in which an individual's identity is apparent or reasonably ascertainable. As highlighted above, browsing history information may not automatically make an individual's identity apparent, especially if the user is not signed in to an online account. In these situations, any browsing aggregation is likely to be conducted around an IP address. Accordingly, whilst it is possible to identify a specific device used for browsing, it may not necessarily mean that the identity of an individual is possible or reasonably ascertainable, as required by the *Privacy Act's* definition of personal information.[94] This has certainly been the argument put forward by organisations which employ direct marketing or behavioural advertising techniques as they have argued that information collected for behavioural targeting cannot be classified as 'personal' for the purposes of the *Privacy Act*.[95] It has also been argued that the use of web proxies[96] and wireless piggybacking prevent IP addresses from being identified with a user or device with total certainty.

However, as has previously been discussed in this research paper, the aggregation of data over time may enable identification of particular individuals and thus render the information personal information. Whilst it is the case that the Privacy Commissioner, has not specifically determined whether an IP address is personal information or not, it should be noted, that both US[97] and Canadian[98] authorities have deemed it so, as has the Queensland Privacy Commissioner in guidance.[99] An IP address on its own is unlikely to be considered personal information. However, if the IP address is used as a means to aggregate data, then it is more likely to be considered personal information as the collation of data around a specific data point will make it more likely that an individual's identity is reasonably ascertainable. Furthermore, the ability to conduct organisational aggregation is

[94] S6(1) Privacy Act 1988 (Cth)
[95] Senate Environment and Communications Reference Committee *The adequacy of protections for the privacy of Australians online,* (7 April 2011) 39 (hereafter 'Senate Environment Committee').
[96] Tools designed to disguise a user's real IP address by assigning them a random alternative. These may also be used to anonymise a user's data by not providing any IP address at all to a given website.
[97] *Klimas v Comcast Cable Communications Inc* 465 F.3d 271
[98] Canadian Federal Privacy Commissioner's findings in PIPEDA Case Summaries #2005-319 http://www.priv.gc.ca/cf-dc/2005/319_20051103_e.cfm and #2009-010 http://www.priv.gc.ca/cf-dc/2009/2009_010_rep_0813_e.cfm at 12 April 2012.
[99] Office of the Information Commissioner, *'IP Addresses, Google Analytics and the Privacy Principles'* http://www.oic.qld.gov.au/files/InformationSheets/Information%20Sheet%20-%20privacy,%20IP%20addresses%20and%20Google%20Analytics.pdf at 12 April 2012.

context specific, that is to say, the ability to aggregate will be judged on a case by case basis that examines the aggregation ability of the organisation in question.[100] This point again re-emphasises the likelihood that the Act would apply to major online marketing or advertising corporations as these organisations will have significant capabilities to undertake sophisticated data aggregation.

If the data collected is deemed to be personal information, then NPP2, which partially relates to direct marketing, is likely to guide where the use of personal information for targeted advertising will be permitted, under certain conditions.[101] Under NPP2 personal information can be used for direct marketing where:

- It is impracticable to obtain consent from individuals;
- The individual must not have made a request not to receive direct marketing; and
- The individual must be informed in each communication of their ability to request the ceasing of the marketing.[102]

The use of Do Not Track mechanisms may be of relevance at his juncture and it raises several questions in relation to NPP2. For example, if an individual has their browser setting to not allow tracking, does that mean they have made a request not to receive direct marketing? Furthermore, if tracking is taking place, does the tracking organisation also have to inform the individual of their ability to request the ceasing of tracking and targeted advertising? These issues have yet to be addressed and it is therefore currently unclear the extent to which the Act applies to online behavioural profiling.

NPP 2 broadly has the effect that any information used or disclosed by an organisation must be within the parameters for which it was collected.[103] It could be argued that the use of web browsing history is collected for the directly related purpose of profiling[104] and it could reasonably be expected that the individual would expect the collecting organisation

[100] See Mark Burdon and Paul Telford, 'The Conceptual Basis of Personal Information in Australian Privacy Law' (2010) 17(1) *Murdoch Elaw Journal* 1, 26.
[101] *Privacy Act 1988*, Schedule 3, NPP 2.1
[102] Ibid.
[103] However, there are a number of exemptions under NPP 2 that provides organisations with much flexibility in interpretation.
[104] NPP 2(a)(i)

would use browsing information for that purpose.[105] However, as studies have demonstrated, the understandings and expectations of individuals in relation to the use of their browsing information for online behavioural profiling are by no means clear.[106] It is therefore equally unclear to what extent NPP2 actually applies to online behavioural profiling and how it applies.

Furthermore, under NPP4.2, an organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed. The application of NPP4.2 is limited in the context of online behavioural advertising as the creation of profiles requires the continued collection and iterative review of previously collected browsing information. Accordingly, online marketers may always find a business use for collected online browsing data which thus negates some of the individual protections afforded by NPP4.2.

One final point should also be noted regarding exemptions to the Act. Since 2000, the *Privacy Act* has made small businesses (defined as those businesses having an annual turnover of $3 million or less) exempt from compliance with its requirements.[107] It is estimated this exemption covers at least 94% of actively trading Australian businesses.[108] Given that a growing number of these businesses are conducting online transactions with customers, holding and using significant quantities of personal information in the process, small businesses operating in the online context pose substantially greater risks to personal privacy in comparison to the old offline model.[109] It is possible therefore that the Act may only apply to large-scale commercial online marketing companies which have an annual turnover of over three million dollars and may not apply to a large number of individual websites that nonetheless collect and track user browsing information.

6 ANALYSIS & RECOMMENDATIONS

In the last substantive section of this research note, a typology of different Do Not Track approaches is put forward to differentiate regulatory frameworks applied in different

[105] NPP 2(a)(ii)
[106] Andrejevic and Arnott above n. 11.
[107] *Privacy Amendment (Private Sector) Act 2000*
[108] Senate Environment Committee, above n. 95.
[109] Ibid, 35.

jurisdictions. The section concludes with an overview of recommendations for improvement.

6.1 TYPOLOGY OF REGULATORY APPROACHES

First, it is necessary to cover some background regarding the development of intra-jurisdictional information privacy law frameworks. The implementations of information privacy laws have taken essentially different tracks despite their similar origins. That in itself is not surprising as a right to privacy is not perceived as an absolute right and thus the interpretation of the emphasis given to an individual's right to control his or her personal information is in competition with other social rights and interests. The application of information privacy legal regimes is likely to be a matter of contestable discussion amongst different legislative jurisdictions.[110] As such, information privacy laws are manifestations of political processes which have implications for the implementable scope of such laws.[111] Jurisdictional information privacy laws therefore reflect the wider social, legal and policy values of individual jurisdictions.[112]

The US attitude towards information privacy law is based on a sectoral regime and as such, is focussed towards certain types of industries or various types of sensitive information.[113] In conjunction with this are a handful of laws that have been implemented that have arisen from specific circumstances, ranging from the use of driver licence information for stalking purposes to the protection of videos borrowed from video stores.[114] Furthermore, these sectoral divisions are emphasised by the fact that some federal privacy laws have been replicated at state level while others have not.[115] Not surprisingly therefore, the US approach to information privacy has been much criticised for its inconsistency of approach

[110] Charles Raab, 'From Balancing to Steering: New Directions for Data Protection' in Rebecca A. Grant and Colin J. Bennett (eds), *Visions of Privacy: Policy Choices for the Digital Age* (University of Toronto Press, 1999) 68.
[111] Colin J. Bennett and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press, [2nd and updated ed, 2006).
[112] Peter P. Swire and Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (Brookings Institution Press, 1998).
[113] Joel R Reidenberg, 'The Globalization of Privacy Solutions: The Movement Towards Obligatory Standards for Fair Information Practices' in Rebecca A. Grant and Colin J. Bennett (eds), *Visions of Privacy: Policy Choices for the Digital Age* (University of Toronto Press, 1999) 217, 209.
[114] *Drivers Privacy Protection Act of 1994* 18 USC § 2725; *The Video Privacy Protection Act of 1998*, 18 USC § 2710.1994.
[115] Joel R. Reidenberg, 'Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?' (1992) 44(2) *Federal Communications Law Journal* 195, 221.

and application, particularly in relation to the manner in which information privacy is dealt with in other regimes as part of a comprehensive legal framework.[116]

Comprehensive frameworks, such as those found in the EU, Canada, New Zealand and Australia, adopt an entirely different approach to the regulation of information privacy – essentially by establishing broad information privacy rights for individuals and stipulating requisite obligations for all organizations regarding the collection, storage and use of personal information. The type of information covered also has wide application and is purposefully construed in a broad sense - see for example, the definition of 'personal data'[117] found in the Data Protection Directive or the definition of 'personal information' detailed in the *Privacy Act*.[118] In conjunction with, supervisory authorities are given a wide discretion to regulate and monitor the actions of organisations and potential infringements against individuals.[119]

It should therefore be no surprise that different jurisdictions have put forward different methods of regulating online behavioural profiling and Do Not Track initiatives.

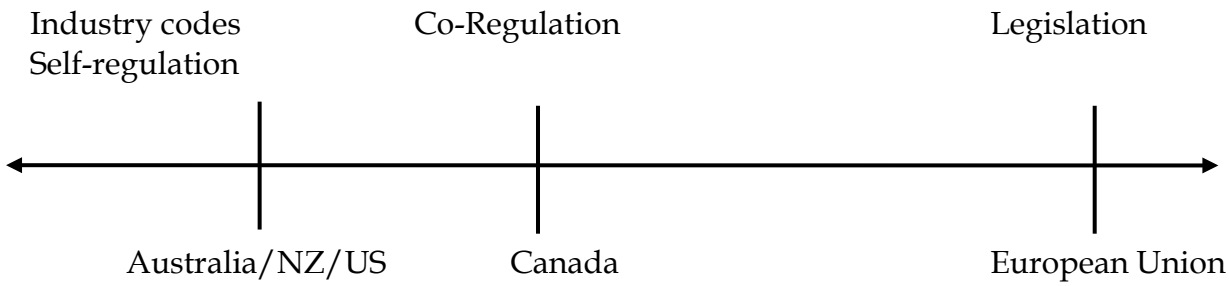
Based on the summary of approaches to online consumer privacy summarised above, three systems of regulatory application can be identified. The first, adopted by New Zealand, Australia and currently the US, is a predominant approach of self-regulation, in which coalitions of advertising companies or companies themselves are responsible for developing and adhering to their own privacy policies and codes of conduct. The second approach is co-regulation which refers to industry self-regulation initiatives that are overseen or ratified by government agencies. Canada is a current example and the US appears to be moving towards this approach as recent legislative proposals assume a much greater oversight role by the FTC. The third approach, adopted by the European Union, is a prescriptive system of mandatory regulation which is enforced by an independent body, typically a data protection commissioner.

---

[116] Robert Gellman, 'Does Privacy Law Work?' in Philip Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (MIT Press, 1997) 193, 195.
[117] *Council Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*
[118] *Privacy Act 1988* (Cth) s 6(1).
[119] Bennett and Raab, above n, 112.

These three systems are not absolute, and no jurisdiction entirely uses one approach to the total exclusion of the other. They can rather be considered a spectrum with self-regulation dominating at one end, and state regulation dominating at the other, as represented by Diagram 1 below.

Diagram 1 – Regulatory Approaches to Do Not Track



Australia has a largely self-regulated industry of targeted advertising. The best example of self-regulation in the Australian context is the *Australian Best Practice Recommendation for Online Behavioural Advertising*, developed by the Australian Association of National Advertisers (ANAA) in March 2011.[120] These recommendations have been designed by stakeholders in the online advertising industry, and are therefore tailored to their desire to engender consumer trust and to provide them the flexibility to carry on their business relatively freely rather than providing meaningful legal protections or redress.

The most frequently raised argument in favour of self-regulation in Australia is that it is the system that can best adapt to and keep up with technological advances.[121] The AANA, in its submission to the Senate Environment and Communications Reference Committee, cited it's Code of Ethics (applicable to all Australian advertisers) to argue that self-regulation 'provides a flexible mechanism to meet the challenges of ever evolving advertising and marketing practices, media environment as well as consumer expectations'[122]. The Communications Council also submitted that its online privacy guidelines and its proposed

[120] Australian Association of National Advertisers, Australian Best Practice Recommendation for Online Behavioural advertising (March 2011).
[121] Senate Environment Committee, above n. 95, 13.
[122] Ibid.

standards on online behavioural profiling are examples of the effectiveness of self-regulation as a tool for enhancing online privacy.[123]

Another perceived advantage of a self-regulatory approach is that it allows those parties with significant interests at stake to have their initiatives accepted or potentially incorporated into legislative amendments dealing with online privacy. Given that it has long been recognised that the challenges posed by online behavioural profiling will most likely require more than just legislative changes, it could be argued that a self-regulatory approach operating in tandem with a strong legislative framework will ultimately be more effective than pure state regulation in providing meaningful privacy protection for online consumers. Such an argument would have the approach adopted by Canada over the EU.

However, a predominantly self-regulatory approach for privacy protection tends to go hand-in-hand with a relatively weak legislative framework, as has been frequently argued about the US legal framework. This statement could also be applied to Australia, where the legislative framework historically lacks meaningful teeth and is practically inapplicable in many instances.[124] Furthermore, the Privacy Commissioner's powers to enforce privacy rights are limited, and there is little capacity to undertake forward looking initiatives, such as the development of industry-wide privacy codes as developed in Canada.[125]

An approach that is too far towards the self-regulated end of the spectrum arguably leaves consumers more vulnerable and dependent on the individual policies and practices of particular organisations.[126] It is frequently claimed by companies such as Google that the risk of organisations acting self-interestedly at the expense of privacy is mitigated by their need to gain the trust of consumers.[127] However, the high number of instances of improper

[123] Ibid, 14.
[124] See Greenleaf, G 'Tabula Rasa: Ten Reasons Why Australian Privacy Law Does Not Exist (2001) 24(1) University of New South Wales Law Journal 262.
[125] Although it should be noted that the federal government has recently proposed to extend the Privacy Commissioner's powers in this way: see Australian Government, First stage response to ALRC Privacy Report, 2009, recommendation 48-1, 89, available at www.dpmc.gov.au/privacy/reforms.cfm at 12 April 2012.
[126] Chris J. Hoofnagle, 'Privacy Self-Regulation: A Decade of Disappointment' in Jane K. Winn (ed), *Consumer protection in the age of the 'information economy'*, Markets and the law (Ashgate, 2006) 379.
[127] Senate Environment Committee, above n. 95, 14.

use of personal data, and the apparent slow speed with which the advertising industry has developed privacy initiatives, must cast at least some doubt on the merits of such claims.[128]

With that in mind, the substantive part of this note will conclude by looking at suggested recommendations to improve the scope of the *Privacy Act* in relation to online behavioural profiling.

6.2 RECOMMENDATIONS FOR AUSTRALIAN DO NOT TRACK INITIATIVES

Both the Senate Environment and Communications Reference Committee Report and the Australian Government, in its response to the ALRC's report, have made a number of proposals to improve the efficacy of Australia's privacy law framework. Those proposals that are relevant to the issue of Do Not Track are detailed briefly below and are supplanted by developments from different jurisdictions.

6.2.1 STRENGTHENING THE SELF-REGULATORY FRAMEWORK

The Senate Environment and Communications Reference Committee found that, at present, many organisations that manage browsers, social networking sites and other web 2.0 sites are exempt from the operation of the *Privacy Act* due to the 'small businesses' exemption. Therefore, in these instances the privacy of Australians' online is largely dependent on the individual policies and practices of particular organisations. In response to the ALRC's report[129], the Australian Government proposed to extend the powers of the Privacy Commissioner to request the development of industry-wide privacy codes where it is considered in the public interest to do so. If such a request was not complied with, the Government also proposed that the Commissioner should be vested with the power to develop and impose an adequate code following consultation with stakeholders.[130] Under these proposals, self-regulation would still largely be the regulatory mode of choice, but it would at least be underpinned by the Privacy Commissioner who could take enforcement actions in circumstances where industry has failed to effectively self-regulate. Such an

[128] Ibid., 26.
[129] ALRC, above n., 90.
[130] Australian Government, above n., 126.

approach is more in line with the co-regulatory methods adopted in Canada and reflects the changes currently taking place in the US.[131]

Those companies currently subject to the Small Business exception under the *Privacy Act* and not party to any self-regulatory regime will face the cost of introducing new privacy infrastructure on their networks, and of training staff in the proper use and protection of consumer information. Thus the economic concerns of Australian business should be considered in the implementation and content of mandatory rules. The self-regulations already adopted by the AANA could provide a basis for future work on a co-regulatory approach as evidenced by developments in the US and Canada.[132]

In many ways, the regulatory approach adopted by the EU provides the highest level of protection for individuals. However, the adoption of such an approach in Australia would require significant amendment to the underlying philosophy and application of info privacy law. For example, the shift from an opt-out approach to an opt-in would in itself have a number of consequences as highlighted by the reluctance of some EU member states to fully implement the E-privacy Directive.[133]

6.2.2 ENHANCING THE POWERS OF THE PRIVACY COMMISSIONER

The change in regulatory focus would also require enhanced powers for the Privacy Commissioner. The Canadian Privacy Commissioner acts as an ombudsman with authority to investigate complaints made by Canadian citizens and report on whether there has been a violation of the Privacy Act or PIPEDA. The Commissioner has also proved willing to become involved in enforcing and auditing the privacy policies of the industry. This is a statutory power conferred by PIPEDA. The Commissioner has also worked with IAB Canada and a variety of online advertising interests to develop a self-regulatory framework for the industry, which was released in August 2011.[134] This framework represents another

[131] Office of the Privacy Commissioner of Canada, *Report on the 2010 office of the Privacy Commissioner of Canada's Consultations on online tracking, profiling, targeting and cloud computing.* http://www.priv.gc.ca/resource/consultations/report_201101_e.pdf, 25 at 12 April 2012.
[132] Australian Association of National Advertisers, Australian Best Practice Recommendation for Online Behavioural advertising (March 2011).
[133] Hogan Lovells, '*EU Modifies Cookie Rules*' http://ehoganlovells.com/rv/ff0001fbca7d4cfee09193f6c241b40f4ea39f24/p=32 at 12 April 2012.
[134] IAB Canada, 'Canada's Advertising Industry Releases Self-Regulation Framework For Online Behavioural Advertising That Ensures Transparency, Education, Choice And Accountability For Consumers' (Press release, 23 August, 2011)

element of cooperation between state and private sectors, having been developed after frequent and extensive consultation with the office of the Privacy Commissioner.[135] Canada therefore offers an example of a jurisdiction in which the protections offered by self-regulation and by state regulation are closely balanced against each other.

It would also appear that successive Canadian Commissioners have been more willing to take a wider view of their role than their Australian counterparts and have demonstrated a greater willingness to become involved in contemporary privacy controversies.[136] The Senate Committee Report, the ALRC and the OAIC[137] itself have recommended that the statutory powers of the Privacy Commissioner be strengthened. It would appear that any substantive change in the law is effectively predicated on the enhancement of statutory powers if Australian privacy law in this area is to have any 'teeth'.

However, it should also be noted that the findings of the Canadian Privacy Commissioner are not legally binding, and therefore in this respect the US enforcement approach, which centres around the FTC protecting consumer rights when organisations breach their own privacy policies, may be the strongest approach to adopt. It should nonetheless be noted that whilst the FTC has developed a meaningful jurisprudence in the area of corporate responsibilities for privacy protection, it cannot not be considered on the same lines as specific information privacy commissions, such as those, in operation in comprehensive information privacy law frameworks.

6.2.3 PROVIDING MEANINGFUL CONSENT

Under the *Privacy Act*, the restrictions on the collection, use and disclosure of personal information can potentially be circumvented in circumstances where the consent of the individual is acquired.[138] The Australian Privacy Foundation submitted to the Senate Environment and Communications Reference Committee that the 'cure-all' effect of consent on individual privacy is not proportionate to the ease with which consent can be obtained.

---

[135] Ibid.

[136] Consider, for example, the findings by the Privacy Commissioner that 'personal information' can, in certain circumstances, include IP addresses and also information stored by temporary and permanent cookies: see Office of the Privacy Commissioner of Canada, above n. 32.

[137] Michael Lee, *Privacy Commissioner Pushes for New Powers* ZDNet <http://www.zdnet.com.au/privacy-commissioner-pushes-for-powers-339319337.htm> at 12 April 2012.

[138] *Privacy Act 1988,* Schedule 3, NPP 2 and NPP 9.

The Foundation gave the example of an individual being forced to 'consent' to "unspecific privacy invasive practices, bundled with pages of other terms and conditions, when signing up for a social networking site"[139] to illustrate this point. The Committee considered that while the *Privacy Act* has allowed for consent to justify the waiver of privacy rights in the offline sphere, perhaps this approach is inappropriate in the online context.[140] Liberty Victoria, made submissions to this effect, arguing that the fundamental differences between offline and online transactions requiring consent rendered the consent justification somewhat untenable for the latter.[141] They pointed to several distinguishing features, including that:

- Australian law often does not cover online transactions, and that consequently the collected data may be used for purposes, or disclosed to other organisations, not envisaged by the consumer;
- Third parties may be collecting the transactional data; and
- Electronic data is rarely deleted, and is more accessible to a greater number of people and organisations than offline data.[142]

In order to meet the challenges presented by online transactions and more effectively deal with complaints about the misuse of privacy consent forms, the Committee recommended an expansion of the Privacy Commissioner's complaint-handling role under s21(1)(ab) of the *Privacy Act.*[143] Additionally, it recommended that the OAIC examine the issue of consent in the online context and subsequently develop guidelines on the appropriate use of privacy consent forms for online services. At present, the OAIC has not developed such a guideline.

As regards other jurisdictions, in terms of offering consumers greater control over the collection, use and disclosure of their personal information, the EU model is the stand-out, because it comprises a comprehensive framework that applies across all industry sectors

[139] APF Submission 14 to the Senate Environment and Communications Reference Committee, 2, cited in Senate Environment Committee, above n. 95, 29.
[140] Senate Environment Committee, above n. 95, 31.
[141] Ibid.
[142] Ibid.
[143] Ibid, 32.

which is enforced by active regulators.[144] Furthermore, it employs an opt-in consent mechanism, which sets a much higher standard to satisfy than the opt-out mechanisms used in Australia, where the default setting is to allow collection and disclosure of personal information until the individual elects to opt-out of such practices. A suggested middle ground could be to require opt-in consent for the collection and dissemination of sensitive information, such as biometric data, race, sexuality, religion, financial and health records. This is arguably a more appropriate approach, as it still allows opt-out consent to operate in many circumstances, but also takes into account the potentially more damaging ramifications of the misuse of sensitive information and thus sets a higher bar for organisations to satisfy if they wish to collect and use such information. A similar approach has also been suggested for US Do Not Track proposals.

6.2.4 REDUCING THE SCOPE OF THE SMALL BUSINESS EXEMPTION

The Senate Committee recommended amendment of the small business exemptions to ensure that those businesses which hold substantial quantities of personal information, or which transfer personal information offshore, are subject to the requirements of the *Privacy Act*.[145] A related recommendation suggested that the *Privacy Act* be amended to provide that all Australian organisations which transfer personal information overseas must ensure that the information will be given at least equivalent protections to those afforded under Australia's privacy framework.[146] These seem practical suggestions to improve the efficacy of the *Privacy Act* in relation to online behavioural profiling.

6.2.5 REGULATING TRANSBORDER INFORMATION FLOWS

One of the inherent limitations when attempting to regulate online behavioural profiling is that the Australian Parliament can only enact privacy laws relating to companies incorporated in Australian or with an Australian link.[147] Regarding the latter, the *Privacy Act* currently applies where the act or practice of an organisation relates to the personal information of an Australian citizen or permanent resident, and the organisation carries on

[144] Mark Burdon, 'Contextualising the tensions and weaknesses of information privacy and data breach notification laws', *Santa Clara Computer & High Technology Law Journal* (2010-2011) 27, 85.
[145] Ibid, 36.
[146] Ibid.
[147] Ibid.

business in Australia and collects or holds the information in Australia.[148] In its submission to the 2010 Senate inquiry into the exposure drafts, the OAIC submitted that the requirement for information to have been collected in Australia is ambiguous, because in a situation where an individual in Australia submits information over the internet to an organisation based overseas, it is uncertain whether the overseas organisation has collected the information at the point of upload (Australia), thereby making it subject to Privacy Act provisions, or whether it has been collected wherever the recipient organisation is based.[149]

Despite the exposure draft amendments attempting to clarify this issue, the Committee recommended that item 19(3)(g)(ii) of the amendments be altered to provide that an organisation has an Australian link if it collects information from Australia, thereby enhancing the scope of the Act's extra-territorial operation to ensure that information collected from Australia in the online context is protected.[150]

The Committee also recommended that the *Privacy Act* be amended so that all Australian organisations that transfer personal information offshore would be fully accountable for protecting the privacy of that information. The Committee was of the view that this would help to avoid situations where small companies could engage in cross-border data transfers with no responsibility to ensure that the privacy of those to whom the information relates would be protected.[151] Again, this could add significant practical protections to data collected from Australian citizens for the purpose of online behavioural profiling.

6.2.6 DEVELOPING A NEW ONLINE PRIVACY STATUTE?

Most of the proposed amendments in the Australian context envisage amendments to the *Privacy Act* rather than the implementation of a new piece of legislation to deal specifically with the unique challenges raised by online privacy protection. While any changes to current online privacy law will necessarily require amendments to the *Privacy Act*, the introduction of an entirely new statute would allow for clarification of the separate rules regarding online privacy as distinct from general privacy. The enormous growth of online

[148] *Privacy Act 1988*, s. 5B
[149] OPC, *Submission to Senate Finance and Public Administration Legislation Committee Inquiry into Exposure Drafts of Australian Privacy Amendment Legislation*, June 2010, 44, cited in Senate Environment Committee, above n. 95, 46.
[150] Senate Environment Committee, above n. 95, 46.
[151] Ibid, 48-49.

behavioural profiling in the last decade and the potential for the further economic expansion of the internet may also necessitate a distinct Online Privacy Act. A more specific act will make the rules related to online privacy easier to find and follow, both for consumers and for businesses. However, such an initiative would require a radical rethink of Australia's privacy law framework given the core principles of Australian privacy law that is enshrined through the *Privacy Act.*

7 CONCLUSION

The issue of online behavioural profiling and Do Not Track legal responses are garnering world-wide interest. Developments are happening at pace and it is likely that some form of US legislation or regulation will be implemented within the next two years. At the same time, ongoing EU developments involving the continuing implementation of the E-Privacy Directive and discussions relating to the new Data Protection Regulation will ensure that the issue of online behavioural profiling will never be far from the policy table. How Australia will respond to these developments is as yet unclear. However, it would appear from global initiatives that there is a distinct move away from predominant self-regulatory approaches to more nuanced, legislative options. Given the global nature of online behavioural profiling, it is likely that Australia will have act in some form or another as maintaining the status quo for the sake of it may not be a viable option.