Chapter 11
Tracking Legislative Developments in Relation to "Do Not Track" Initiatives

Brigette Garbin
University of Queensland, Australia

Kelly Staunton
University of Queensland, Australia

Mark Burdon
University of Queensland, Australia

ABSTRACT

Online behavioural profiling has now become an industry that is worth billions of dollars throughout the globe. The actual practice of online 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. Consequently, it should be no surprise that legislative initiatives are afoot throughout the world including the United States (US), the European Union (EU), and Australia. These different jurisdictions have put forward different methods of regulating online behavioural profiling and Do Not Track initiatives. Accordingly, this chapter overviews legislative developments and puts forward a typology of different legislative initiatives regarding the regulation of online behavioral profiling and Do Not Track issues. Particular focus is given to the Australian situation and whether existing Australian privacy law is sufficient to protect the privacy interests of individuals against the widespread use of online behaviour profiling tools.

INTRODUCTION

"Do Not Track" initiatives have emerged as a popular legislative response to the difficult problem of privacy concerns in relation to online behavioural profiling. For example, 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

DOI: 10.4018/978-1-4666-4582-0.ch011

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. At present, little action has taken place in Australia but given the worldwide interest in "Do Not Track" it would seem unlikely that inaction will suffice.

Consequently, this Chapter examines current legal initiatives to identify the complex issues that arise out of online behavioural profiling and subsequent Do Not Track proposals. The second section provides an overview of how online behavioural profiling operates, the privacy concerns that arise and highlights recent contemporary controversies. The next two sections detail Do Not Track legislative initiatives that have recently taken place in the United States (US) and outline developments in the EU, Canada and New Zealand. These are followed by an overview of recent Australian developments while the final section 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.

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" (Federal Trade Commission [FTC], 2009). The actual practice of tracking was once limited to the installation of traditional cookies that record the websites a user visits (Wall Street Journal, n.d.). 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 (Electronic Privacy Information Centre [EPIC], n.d.).*Third party cookies* are the primary mechanism used for online tracking. These cookies are operated by a "third party", the advertising or marketing 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 user based on their browsing activities that is subsequently used for the purpose of delivering targeted advertisements (Duhig, 2012). Online behavioural tracking has become a burgeoning industry precisely because of the potency of advertising that it provides for (Phillips, 2010). 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