Profiling the Mobile Customer – Is Industry Self-Regulation Adequate to Protect Consumer Privacy When Behavioural Advertisers Target Mobile Phones? – Part II

Computer Law and Security Review September 2010

King, Nancy J.
College of Business, Oregon State University, U.S.A.

Jessen*, Pernille Wegner
Aarhus School of Business, Aarhus University, Denmark
*Corresponding Author

Citation for final version published by Elsevier: King, N. J., & Jessen, P. W. (2010). Profiling the mobile customer – Is Industry Self-Regulation Adequate to Protect Consumer Privacy When Behavioural Advertisers Target Mobile Phones? – Part II. *Computer Law and Security Review*, *26*(6), 595-612. doi:10.1016/j.clsr.2010.09.007

Part II, Profiling the Mobile Customer – Is Industry Self-Regulation Adequate to Protect Consumer Privacy When Behavioural Advertisers Target Mobile Phones?

Nancy J. King
College of Business, Oregon State University, U.S.A.

Pernille Wegener Jessen*
Aarhus School of Business, Aarhus University, Denmark
*Corresponding author

Abstract: Mobile customers are increasingly being tracked and profiled by behavioural advertisers to enhance delivery of personalized advertising. This type of profiling relies on automated processes that mine databases containing personally-identifying or anonymous consumer data, and it raises a host of significant concerns about privacy and data protection. This second article in a two part series on "Profiling the Mobile Customer" explores how to best protect consumers' privacy and personal data through available mechanisms that include industry self-regulation, privacy-enhancing technologies and legislative reform.[1] It discusses how well privacy and personal data concerns related to consumer profiling are addressed by two leading industry self-regulatory codes from the United Kingdom and the U.S. that aim to establish fair information practices for behavioural advertising by their member companies. It also discusses the current limitations of using technology to protect consumers from privacy abuses related to profiling. Concluding that industry self-regulation and available privacy-enhancing technologies will not be adequate to close important privacy gaps related to consumer profiling without legislative reform, it offers suggestions for EU and U.S. regulators about how to do this.[2]

Keywords: consumer profiling, behavioural advertising, targeted marketing, mobile phones, mobile commerce, privacy, data protection, sensitive data, industry self-regulation, fair information practices, privacy-enhancing technologies.

1. Introduction

Data protection issues arise when data mining is used to process mobile phone users' personal data and to create customer profiles for targeted marketing purposes. Even when profiling does not use personal data and thus may not be regulated under data protection laws, more traditional privacy concerns about whether profiling unduly interferes with consumers' personal autonomy and liberty arise. Potential harms from consumer profiling encompass: 1) interference with consumers' rights of data protection, including the right to adequate notice and to give consent for personal data collection and processing; 2) being subjected to pervasive and non-transparent commercial tracking; 3) increased generation of unwanted commercial solicitations (spamming); 4) increased exposure to data security risks such as identity theft and fraud; and 5) increased exposure to potential types of unfair commercial practices such as unfair offer or price discrimination. For consumers, profiling is not likely to be transparent making it difficult to identify the source of any privacy harms, especially if they do not have access to meaningful information about the profiles that have been generated about them.

Regulatory frameworks in both the EU and U.S. include privacy, data protection and consumer protection legislation. However, regulators have not yet fully addressed the privacy and data protection challenges associated with profiling the mobile customer. Specific data protection and privacy gaps exist under both the EU and U.S. regulatory frameworks leaving consumers vulnerable in the context of profiling by behavioural advertisers ("privacy gaps"). These privacy gaps include: 1) uncertainty about whether IP addresses, cookie data and other secondary identifiers are personal data which may be used to build consumer profiles; 2) whether consumers are entitled to

[1] See the first article in this series on *Profiling the Mobile Customer*: King, N.J. and Pernille Wegener Jessen, 'Profiling the mobile customer – Privacy concerns when behavioural advertisers target mobile phones,' Part I, *Comput. Law and Secur. Rev.* (2010).

[2] The article is related to the research project *Legal Aspects of Mobile Commerce and Pervasive Computing: Privacy, Marketing, Contracting and Liability Issues* funded by the Danish Council for Independent Research; Social Sciences. See further information on the project, at: http://www.asb.dk/article.aspx?pid=19387.

access meaningful information about profiles that relate to them; 3) whether applying a group profile to an individual creates personal data, especially if no other personal data is used in creating the profile; 4) how the concept of sensitive personal data should be applied to consumer profiling; 5) whether creation and use of some profiles for market segmentation purposes may be so sensitive that stronger privacy protections are merited; and 6) the need to prevent and redress particularly unfair or discriminatory forms of consumer profiling. Recent developments such as the Draft Recommendation on Profiling from the Council of Europe, amendments to the EU's E-Privacy Directive that further restrict placing tracking cookies on consumers' computers, an opinion by the Article 29 Data Protection Working Party on behavioural advertising and self-regulatory guidelines on fair information practices for behavioural advertisers from the U.S. Federal Trade Commission provide insights into the type of consumer privacy protections that are needed.

Having discussed the above matters in the first article in this series, this second article tackles the question of how to close the current privacy gaps related to consumer profiling and specifically what regulation is needed to adequately protect mobile consumers' privacy and personal data. It considers government and non-government mechanisms to protect consumers' privacy including industry self-regulation, privacy-enhancing technologies and legislation. The article compares two leading self-regulatory codes from the United Kingdom and the U.S. that have been developed by industry associations for use by their members engaged in behavioural advertising. Concluding that industry-self regulation and privacy-enhancing technologies currently do not adequately protect consumers' privact with respect to profiling by the behavioural advertising industry, it makes suggestions for legislative reform to close the privacy gaps in the current EU and U.S. regulatory frameworks.

Since it is possible that legislative reform to address profiling by behavioural advertisers would unduly burden this new industry, perhaps stifling its growth without offsetting consumer profiling benefits, the search for solutions to protect consumers' privacy with respect to profiling naturally begins with consideration of alternatives.

2. Self-regulatory Mechanisms to Protect Consumers' Privacy.

Those considering the adequacy of existing privacy and data protection laws and whether there is a need for legislative reform should consider the privacy protections consumers already have due to self-regulatory mechanisms that are in place for this purpose, assuming they are effective. In assessing the adequacy of existing privacy and data protection legislation, it has been persuasively argued that a "technology-assessment" approach is needed that gives "better attention to the solution the technology itself might offer."[3] There are at least three self-regulatory mechanisms that could be adopted by behavioural advertising companies that potentially would protect consumers' privacy and personal data: 1) conducting privacy impact assessments to identify relevant privacy and data protection concerns; 2) addressing these concerns through potential privacy-enhancing technologies, and/or 3) addressing these concerns by adopting company or industry privacy policies that commit to fair information practices.

A brief overview of three primary self-regulatory mechanisms is provided in this section as a prelude to examining two different industry self-regulatory codes that have been adopted by behavioural advertisers in the UK and the U.S. for their members. These three mechanisms of self-regulation can work together or separately to protect consumers' privacy and personal data.

2.1 Privacy Impact Assessments. A privacy impact assessment (PIA) "is usefully defined as a process whereby a project's potential privacy issues and risks are identified and examined from the perspectives of all stakeholders, and a search is undertaken for ways to avoid or minimi[z]e privacy concerns."[4] The process of conducting a PIA should include consideration of the application of fair information practices to profiling by behavioural advertisers and

[3] Poullet, Y., 'Data protection legislation: What is at stake for our society and democracy?' 25 *Comput. Law and Secur. Rev.*, pp. 211-226 (2009).

[4] Information Commissioner's Office, United Kingdom, Privacy Impact Assessment Handbook, Version 2.0 (ICO PIA Handbook), available at: http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html (last accessed, 23 July 2010). A PIA aims to prevent problems from a privacy perspective and is best undertaken at an early stage in a project and is distinguished from a privacy audit (which is after-the-fact) or a legal compliance audit.

whether there are any specific privacy concerns for mobile customers. [5] For example, the PIA should specifically address delivery of targeted advertising to consumers with mobile phones and the personalization and localization of profiling that is possible due to availability of geographic location data and other features of mobile phone use. A PIA should also consider the availability of privacy-enhancing technologies that could protect consumer's privacy.

2.2 Privacy-Enhancing Technologies. A Privacy-Enhancing Technology (PET) is something that reduces or eliminates the risk of contravening privacy principles and legislation, minimises the amount of data held about individuals, or empowers individuals to retain control of information about themselves.[6] PETs encompass "technical and organisational concepts" that aim to protect a consumer's identity and often involve encryption in the form of "digital signatures, blind signatures or digital pseudonyms."[7] A primary advantage of PETs is that they may offer anonymity to those in mobile commerce, enabling consumers to participate without revealing their identities or otherwise providing PII.[8] However, location data that has been processed to prevent discovery of the geographic location of mobile devices may not reliably prevent discovery of this information.[9]

Another potential technological solution, Platform for Privacy Preferences ("P3P") was proposed to protect consumer privacy in e-commerce.[10] P3P is software designed to monitor website privacy policies. Conceptually, with P3P, websites post their practices in a "standard format that can be retrieved automatically and interpreted easily by user agents." [11] A user then may choose which websites are allowed to track the user based on each

---

[5] According to David Flaharty, "privacy impact assessments … can be customised to the needs of any organisation. The essential goal is to describe personal data flows as fully as possible so as to understand what impact the innovation or modification may have on the personal privacy of employees or customers and how fair information practices may be complied with." Flaherty, D., 'Privacy Impact Assessments: An Essential Tool for Data Protection,' 7 *Privacy Law and Policy Reporter,* p. 85 (2000), available at: http://www.austlii.edu.au/au/journals/PLPR/2000/45.html (last accessed, 23 July 2010).

[6] Information Commissioner's Office, United Kingdom, Privacy by Design, p. 8 (Nov. 2008), available at: http://www.ico.gov.uk/upload/documents/pdb_report_html/privacy_by_design_report_v2.pdf (last accessed, 23 July 2010).

[7] Solove, Daniel J., Rotenberg, Marc and Schwartz, Paul, *Information Privacy Law*, p. 624 (2nd ed., 2006) (Solove et al.) (internal quotations omitted). According to Camp and Osorio "privacy-enhancing solutions for e-commerce are technical representations of a perception of the meaning of privacy… [which] are the result of the interaction between a specific bias toward privacy and the capacity to build specific technology within the framework created by current business practices." Arguing privacy is a critical element of trust in e-commerce, Camp and Osorio articulate three specific concepts of privacy (privacy as rights of autonomy, seclusion or property) that are transformed into technical representations of the meaning of privacy through privacy-enhancing solutions for e-commerce. Camp, J. and Osorio, C., 'Privacy-Enhancing Technologies for Internet Commerce,' John F. Kennedy School of Government, Harvard University, Faculty Research Working Papers Series 7-8, August 2002, available at: http://ideas.repec.org/p/ecl/harjfk/rwp02-033.html (last accessed, 23 July 2010).

[8] Privacy-enhancing location-based services (LBS) for conventional deployment (which typically involves a mobile operator and a LBS service application provider) have been proposed to give users more control over their personal data. See Kosta et al., 'Legal Considerations on Privacy-Enhancing Location Based Services Using PRIME Technology,' 24 *Comput. Law and Secur. Rep.,* pp. 139-46 (2008). Privacy-enhancing LBS systems using a PRIME toolbox enhance the privacy of users by involving an intermediary that decouples the mobile operator and the LBS service application provider, thus allowing mobile users to receive LBS without unnecessarily disclosing their identities or unnecessarily giving access to personal data that could be used to create excessive consumer profiles. Ibid.

[9] Goodin, D., 'Scrubbed geo-location data not so anonymous after all,' *The Register* (21 May 2009), available at: http://www.theregister.co.uk/2009/05/21/geo_location_data (last accessed, 23 July 2010).

[10] Solove et al., note 7, p. 642.

[11] Ng, H., 'Targeting Bad Behavior: Why Federal Regulators Must Treat Online Behavioral Marketing as Spyware,' 31 *Hastings Communications and Entertainment Law Journal*, p. 385 (2009)(Ng)(difficulties for the user include being required to spend time managing their privacy preferences including making choices on transaction-by transaction and the fact that Websites would not be required to participate, so some Websites participating in OBA may not allow the preset privacy preferences of the user to be followed).

website's privacy policy, which the user's web browser checks against the privacy preferences preset by the user. Although P3P was designed for traditional e-commerce, P3P could become an effective tool to help mobile consumers exercise choices related to privacy policies associated with profiling by behavioural advertisers provided the technology is made compatible with the mobile environment.[12] Despite its anticipated potential, currently many major websites do not use P3P to summarize their privacy policies. It is argued that P3P has become irrelevant and new tools are needed to help consumers understand privacy policies posted by websites. To meet this need, Mozilla Foundation, provider of the Firefox web browser, is designing a standard set of colored icons to reveal how data protective or intrusive websites are so that consumers concerned about their privacy will not have to read legalistic privacy policies.[13] This effort is still in infancy.

Companies conducting behavioural advertising typically use a combination of web tracking technologies and cookie technologies to enhance their ability to deliver highly personalized advertisements. Cookies are used to identify the user of a website and web beacons and similar technologies track the user's behaviour on the site.[14] Web beacons may report site traffic, count unique visitors and audit advertising. Web beacons can record almost every move of a website user. Because sensitive information about a user's lifestyle or interests may be inferred from information gathered through this type of tracking, significant privacy concerns are raised.[15] Users do not have any control over web beacons as they reside on websites that users visit rather than on the users' computers. In contrast, users can set their browsers to accept or reject cookies and can delete cookies by using their browsers or anti-spyware programs.[16]

PETs specifically designed to protect consumers' privacy in the context of behavioural advertising have been proposed to give consumers greater control over whether or not to have their information collected for this purpose. For example, modification of the technical design of cookies has been proposed.[17] Downloaded to the user's computer (or other device such as a mobile phone), cookies are currently the primary mechanism for a website engaged in behavioural advertising to determine if the same computer is returning to the website and to recognize the user's choice about whether or not to participate in behavioural advertising. To facilitate consumer privacy, cookies need to be designed that will uphold consumer choice with respect to behavioural targeting, with the design of both "opt in" and "opt out" cookies being technically feasible to support consumers who choose not to participate in behavioural profiling. Currently, however, "opt out" cookies are often deleted by anti-spyware software, allowing targeting to resume by the same websites that the consumer has opted out of being tracked. To fix this problem, anti-spyware technology needs to be modified to honor opt out cookies in order to respect the consumer's choice not to be tracked.[18] Additionally, "opt out" cookies are often deleted when consumers use their Internet browser software

---

[12] Cleff, E.B., 'Implementing the Legal Criteria of Meaningful Consent in the Concept of Mobile Advertising,' 23-3 *Computer Law & Security Report*, pp. 267-68 (2007) (Cleff, CLSR) (reporting on a project called Privacy in Mobile Internet (PIMI) that has the objective of developing an advising privacy platform for small displays like those found on mobile phones).

[13] McCullagh, D., 'Mozilla weighs privacy warnings for Web pages,' *CNETcom* (2 Feb. 2010), available at: http://news.cnet.com/8301-13578_3-10445642-38.html (last accessed,23 July 2010).

[14] Gilbert, F., 'Beacons, Bugs and Pixel Tags: Do You Comply with the FTC Behavioral Marketing Principles and Foreign Law Requirements,' *Journal of Internet Law,* p. 4 (May 2008) (describing web beacons, action tags, clear GIFs, web tags, pixel tags, web bugs and similar tracking technologies as small strings of software code used for behavioural advertising that differ from cookies because they are inconspicuous to the user – their presence can be identified only by examining the website code and they cannot be removed or deactivated by the user because they do not reside on the user's computer).last accessed,

[15] Gilbert, note 13, p. 4..

[16] Ibid.

[17] Comments, Swire, P. and Anton, A., "In regard to the FTC Staff Statement, 'Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles,'" Federal Trade Commission, p.2 (10 Apr. 2008) (Comments on FTC Staff Statement), available at: http://www.ftc.gov/os/comments/behavioraladprinciples/080410swireandanton.pdf (last accessed, 23 July 2010).

[18] For anti-spyware companies to be able to recognize opt out cookies, criteria or standards for defining "opt out cookies" would need to be developed. If anti-spyware companies recognize opt out cookies and their software does not delete them from users' computers, this gives rise to a security risk that other sorts of cookies might be disguised

to delete all cookies, and so browser software needs to be updated to enable consumers to manage their opt out cookies more effectively.[19] Modification of anti-spyware software and browser software for the above purposes would make cookies a much more effective tool to facilitate consumer choice about behavioural targeting.

Some browser software makers have announced they are designing new features for their Internet browsers that will include tools to allow a user to anonymously surf websites by directing his or her browser not to save browsing and searching history, cookies, form data or passwords and to automatically clear the user's browser cache at the end of each session.[20] Alternatively, truly private browsing can be conducted through at least one search engine that offers a proxy service, although it is slower to load and doesn't allow the surfer to enter information in forms, making it less than desirable for e-commerce transactions.[21] Further, browser add-on features are being developed to give users the ability to "lock out" targeted advertising by the leading advertising networks.[22] These technologies are just being developed and are not yet widely in use. The development of privacy-enhancing features for Internet browsers could substantially empower users to limit behavioural advertising by preventing cookies from being placed on their computers, although user education would likely be required. On the other hand, a recent study shows some online tracking tools allow websites to circumvent users' ability to opt out of online tracking. These tools enable tracking for profiling by extracting identification information from users' Internet browsers without the necessity of placing cookies on the users' computers.[23] The ability of behavioural advertisers to track consumers even when they have eliminated cookies from their hard drives means effective PETs have not yet been designed to enable consumers to exercise their choice about whether to be tracked and profiled by behavioural advertisers.

Some argue it is important to make a distinction between Transparency-Enhancing Technologies (TETs) and the broader concept of PETs to help focus consumer privacy discussions related to profiling by behavioural advertisers, arguing it is transparency, rather than anonymity, that consumers most need in this context.[24] For example, when

---

as opt out cookies in order to avoid being deleted. A public white list for opt out cookies has been recommended as a possible solution for this security risk. Comments on FTC Staff Statement , p. 7.

[19] Comments on FTC Staff Statement , note 17, p. 7 (suggesting that browser settings be updated to handle opt out cookies better, for example allowing users to set opt out cookies and to have opt out cookies remain in place when other cookies are deleted).

[20] Keizer, G., 'Microsoft Adds Privacy Tools to IE8,' *ComputerWorld.com* (25 Aug. 2008); Blog posting by Polonetsky, J., Firefox soon to dent behavioural advertising? New plans for third-party cookies,' Future of Privacy Forum (3 June 2010), at: http://www.futureofprivacy.org .

[21] Start.page.com, is such a private search engine offered by Ixquick.com, at: www.ixquick.com (last accessed,23 July 2010).

[22] Kirk, J.,'Browser Add-on Locks out targeted Advertising,' *PCWorld.com*. (17 Mar. 2009) (announcing Targeted Advertising Cookie Opt Out (TACO) which enables its users to opt out of 27 advertising networks that are employing behavioural advertising systems by setting permanent opt out cookies for Google's network and 26 others), available at: http://www.pcworld.com/businesscenter/article/161380/browser_addon_locks_out_targeted_advertising.html (last accessed,23 July 2010).

[23] See Eckersley, P., 'How Unique is Your Web Browser?,' Electronic Frontier Foundation, p. 4 (undated), in Comments of the Electronic Frontier Foundation Before the Federal Trade Commission, Washington, D.C. (2 Mar. 2010) (discussing how device fingerprints are a "means to distinguish machines behind a single IP address, even if those machines block cookies entirely") (Eckersley), available at: http://www.ftc.gov/os/comments/privacyroundtable/544506-00106.pdf (last accessed, 23 July 2010); Davis, W., 'EFF Shows How Companies Can Track Cookie-Deleters,' *MediaPostBlogs* (29 Jan. 2010) (reporting that Peter Eckersley says "once Web sites collect browser 'fingerprints,' then those sites can theoretically recognize some visitors upon their return regardless of whether they still have their cookies," and "sites that identify a returning browser based on the configuration data – or , perhaps a combination of configuration data and IP address – can then restore any cookies previously associated with that browser."), available at: http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=121599 (last accessed, 23 July 2010).

[24] Hildebrandt, M., 'Profiling into the Future: An Assessment of Profiling Technologies in the Context of Ambient Intelligence,' 1 *FIDIS Journal of Identity in the Information Society*, pp. 2-3, 9–11, 12-13, 16-17 (2007), available

businesses use computer profiling to provide targeted services to customers, Mireille Hildebrandt argues that providing adequate transparency means giving consumers access to the profiles that are being applied to them so that they have the opportunity to assess the impact of profiling on their lives.[25] While PETs designed to protect consumer privacy will naturally focus on hiding data and on the use of pseudonyms that will enable consumers to be anonymous in the presence of behavioural advertising, Hildebrandt argues these types of technological protections for privacy will not be adequate to minimize the privacy risks associated with profiling because consumers will need more than just the ability to avoid identification.[26] Instead of anonymity, she argues that what consumers will need to protect their privacy is transparency in the form of access to the profiles that are used with respect to them. This means that effective TETs must be put into place to address the real privacy issue – the generation of highly sophisticated group profiles that are applied in nontransparent ways that significantly impact the autonomy of those profiled.[27] Effective TETs have not yet been invented.[28]

2.3 Industry Codes or Company Privacy Policies. These codes and policies explain the information practices that industry associations or individual companies have promised to follow for the collection, processing, and distribution of individuals' personally identifying information.[29] In mobile commerce, privacy codes and policies give notice of an organisation's privacy practices to consumers, including notice to those who are on the receiving end of behavioural advertising. The extent to which an industry's code of conduct or a company's privacy policy complies with fair information principles advocated or adopted by various organisations is a measure of how well that policy is designed to protect the personal data and privacy of individuals. A company may also seek TRUSTe or BBBOnLine privacy certifications to signify that the company is following the privacy standards to which it has agreed and qualifies for the right to display these privacy seals of approval on their websites.[30]

There is a growing consensus among privacy experts that complex privacy policies contained in a single document are not an effective way to communicate with consumers about the information processing practices of a business.[31] Instead, privacy policies that feature more than one layer of consumer notices, from short notice forms to longer notice forms, are generally viewed as more effective methods to communicate privacy policies.[32] In determining

---

at: http://www.fidis.net/fileadmin/journal/issues/1-2007/Profiling_into_the_future.pdf (alteration in original) (last accessed,23 July 2010).

[25] Hildebrandt, note 24, pp. 15-17.

[26] Hildebrandt, note 24, p. 17

[27] Ibid.

[28] Hildebrandt, M. and Gutwirth, S. (eds.), *Profiling the European Citizen, Cross-Disciplinary Perspectives*, Springer, p. 367 (2008) (Profiling the European Citizen) (according to Mireille Hildebrandt and Serge Gutwirth "we will need transparency enhancing tools (TETs)" to "empower citizens to unfurl the profiling operations they are subject to"; "TETs, however, are still to be invented ….").

[29] Ciocchetti, C., 'E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors,' 44 *American Business Law Journal*, p. 68 (2007) (Ciocchetti, ABLJ, 2007).

[30] See Hewlett Packard Company's online privacy statement that has been validated by TRUSTe Web Privacy Seal Program (TRUSTe) and the Better Business Bureau Online Privacy Program (BBBOnLine), at: http://welcome.hp.com/country/us/en/privacy.html (last accessed,23 July 2010).

[31] See Center for Information Policy Leadership, Ten Steps to Develop a Multilayered Privacy Notice 1–9 (Mar. 2007), http://www.hunton.com/files/tbl_s47Details%5CFileUpload265%5C1405%5CTen_Steps_whitepaper.pdf (last accessed,23 July 2010); Martin Abrams et al., Memorandum, Berlin Privacy Notices (Apr. 2004) (Berlin Privacy Memorandum), available at: http://www.hunton.com/files/tbl_s47Details/FileUpload265/681/Berlin_Workshop_Memorandum_4.04.pdf (last accessed,23 July 2010).

[32] According to privacy experts, whether the notice is provided online or in paper form, a short initial privacy notice should be provided to the consumer that discloses: "(1) Who is covered by the privacy notice (i.e., who is the responsible person or entity); (2) The types of information collected directly from the individual and from others about the individual; (3) Uses or purposes for the data processing; (4) The types of entities that may receive the information (if it is shared); (5) Information on choices available to the individual to limit the use and/or exercise of any access or other rights, and how to exercise those rights; and (6) How to contact the data collector for more

whether a code or policy conveys appropriate notice of privacy practices, it is important to look at the nature of the medium on which the privacy disclosures are made and on which the consumer will convey his or her consent. Since the viewing screen on most mobile phones is very small, the possibility of using multilayered privacy policies, as opposed to a comprehensive stand-alone code or policy, is especially relevant in this discussion of obtaining appropriate consent for behavioural advertising.[33] Websites are starting to display icons to indicate that behavioural advertising is taking place on their sites and that the participating advertisers adhere to an industry code of self-regulatory rules to assure organizations provide fair information practices and protect consumers' privacy.[34]

Privacy policies are posted on many websites engaged in behavioural advertising making it seemingly easy for consumers to be informed about the use of their personal information and enable them to make choices. However, these privacy policies have been criticized as difficult for consumers to understand and inadequate because they include provisions that permit abuse by marketers. Examples of inadequate privacy policies include Pay Pal's privacy policy that allows it to collect additional information "from or about you in other ways not specifically described here" and DoubleClick's policy that states that it can change the policy at any time.[35] Further, in the absence of adequate privacy legislation, consumers lack the bargaining power to obtain better privacy protections. This is so because behavioural advertising usually arises under nonnegotiable user agreements or policies that give consumers little recourse if they do not agree to the website or marketers' terms other than to choose not to use a particular website or search engine.[36] As discussed in the first article in this series, EU privacy and data protection laws provide minimum protections for consumers that cannot be undercut by such privacy policies, but no generally applicable U.S. laws exist that provide similar privacy protections.

This article now discusses two examples of industry self-regulatory codes that are designed to define fair information practices and set privacy standards for behavioural advertising by companies that are members of the industry associations that created the codes. The goal of this section is to assess whether these self-regulatory codes adequately address the privacy gaps related to consumer profiling by behavioural advertisers.

3. Leading EU and U.S. Industry Self-Regulatory Codes

Two industry associations, the Internet Advertising Bureau (IAB)[37] and the Network Advertising Initiative (NAI)[38] have self-regulatory codes for their members engaged in online behavioural advertising (OBA).[39] These two sets of

---

information and how to make a privacy complaint (to the collector and to an independent oversight body, if appropriate). Berlin Privacy Memorandum, note 31, p. 2.

[33] Models for short privacy notices that could be delivered on the screen of a mobile phone have been proposed, including one only four lines long, as follows: (1)the company has a privacy policy, (2)"We collect your information to market to you and to service your account," (3)"You may tell us not to do so," and (4)"View our complete privacy policy by calling [telephone number] or at [Website address]." Ciocchetti, ABLJ (2007), note 29, p. 102 (fig.1).

[34] Davis, W., 'Agencies Test Industry's new "You are Being Targeted" Icon, *Online Media Daily* (26 Mar. 2010), available at: http://www.mediapost.com/publications/?fa=Articles.printFriendly&art_aid=124994 (last accessed,23 July 2010); 'UK could get icons on behavioural ads,' *Out-Law News* (3 Feb. 2010, updated 4 Feb. 2010) (reporting the UK's Interactive Advertising Bureau is working with industry associations in the U.S. that developed an icons to notify consumers about behavioural advertising and hopes they will be adopted in the UK, across the EU and that eventually a consistent global icon will be established), available at: http://www.out-law.com/page-10727 (last accessed, 23 July 2010).

[35] Ng, note 11, pp. 377-378.

[36] Ibid.

[37] Internet Advertising Bureau, Good Practice Principles for Online Behavioural Advertising (IAB Principles), (undated), available at: http://www.youronlinechoices.co.uk/wp-content/uploads/2010/01/IAB-UK-Good-Practice-Principles-for-Online-Behavioural-Advertising.pdf (last accessed,23 July 2010).

[38] Network Advertising Initiative, '2008 NAI Principles, The Network Advertising Initiative's Self-Regulatory Code of Conduct' (2008) (NAI Code), available at: http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf (last accessed,23 July 2010).

self-regulatory guidelines allow comparison of approaches to industry self-regulation by behavioural advertisers in the EU and the U.S.

[Insert Exhibit 1 about here --chart comparing IAB Principles and NAI Code discussed in this section]

3.1 The IAB's Good Practice Principles. This code from the United Kingdom is a leading example of self-regulation by behavioural advertisers, reflecting the more comprehensive regulatory framework for data protection found in the EU. The IAB's Principles bind IAB members prospectively with regard to their operations in the UK.[40] The Principles reference the UK's data protection law and the UK's electronic communications regulations.[41] There are three basic IAB Principles: Notice, Choice and User-Education.[42] Both first-party (OBA by the website the data subject is visiting) and third-Party (OBA by other parties such as network advertising partners) are covered. However, the Principles do not address contextual advertising (OBA based on a single visit or search query), although, of course, EU data protection laws as implemented in UK data protection laws would still apply to processing of PII for contextual advertising purposes. The IAB Principles require opt out consent as a minimum and specify that more robust consent may be required to use PII or sensitive personal data, deferring to the Data Protection Directive's requirement of explicit consent for the use and sharing of sensitive data.[43] Members are required to give users clear and understandable information in their privacy policies about how to control and delete cookies and must provide opt out tools.[44]

---

[39] Additionally, separate cross-industry guidelines were recently put forth by leading marketing and advertising industry groups that include the American Association of Advertising Agencies, the Association of National Advertisers (administered by the Council of Better Business Bureaus), and the Direct Marketing Association. 'Self-Regulatory Principles for Online Behavioral Advertising,' July 2009 (Cross Industry Guidelines), available at: http://www.iab.net/media/file/ven-principles-07-01-09.pdf (last accessed,23 July 2010). See also, 'Key Advertising Groups to Develop Privacy Guidelines for Online Behavioral Advertising Data Use and Collection,' *IAB.net*, 13 January 2008, available at: http://www.iab.net/insights_research/530468/iab_news/iab_news_article/634777 (last accessed,23 July 2010); Clifford, Stephanie "Industry Tightens Its Standards for Tracking Web Surfers," *The New York Times* (1 July 2009), available at: http://www.nytimes.com/2009/07/02/business/media/02adco.html (last accessed,23 July 2010). Critics of the Cross Industry Guidelines believe it omits key privacy protections for consumers. For example, Saul Hansell argues the Cross Industry Guidelines "largely codifies the practices engaged in today" by behavioural advertisers without "endorsing any of the ideas that have been actively discussed recently that might give users more meaningful information and control over how their behavior is being tracked." Hansell, S., 'Four privacy Protections the Online Ad Industry Left Out,' *The New York Times*, 6 July 2009, available at: http://bits.blogs.nytimes.com/2009/07/06/four-privacy-protections-the-ad-industry-left-out/ (last accessed,23 July 2010). Hansell summarizes four consumer privacy protecting ideas that were not adopted in the Cross Industry Self-Regulatory Guidelines: "Every ad should explain itself; Users should be able to see data collected about them; Browsers should help enforce user choices about tracking; [and] some information is simply too sensitive to track." Because the Cross Industry Guidelines adds little of substance to the discussion that has not already been covered by the FTC Guidelines, the NAI Code and the IAB's Good Practice Principles, it is not analysed further in this article. Federal Trade Commission, 'Self-Regulatory Principles For Online Behavioral Advertising,' February 2009 (FTC Guidelines), available at: http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf (last accessed,23 July 2010).

[40] IAB Principles, note 37 ("Meeting IAB Principles, Compliance").

[41] IAB Principles, note 37, Annex 1 (reporting that Phorm, a company engaged in online behavioural advertising, is a signatory to the IAB Principles). See also, Telecoms: The Commission launches case against UK over privacy and personal data protection, IP/09/570, (reporting that the European Commission has started legal action over the online advertising technology of Phorm, claiming Phorm "intercepted" user data without clear consent and that the UK needs to review its online privacy laws), available at: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570 (last accessed,23 July 2010).

[42] IAB Principles, note 37, (Principles 1, 2 and 3).

[43] IAB Principles, note 37, (Guidance Note 4). See also Article 8(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, 23.11.95 (Data Protection Directive). Special categories of processing are defined by Article 8 and are referred to in this paper as sensitive personal data.

[44] IAB Principles, note 37 (Guidance Note 3).

With respect to profiling the mobile customer, there are critical weaknesses in the IAB's Principles starting with failure to directly explain that behavioural advertising involves customer profiling, failure to describe what profiling entails, and failure to address how profiling by behavioural advertising relates to mobile customers. Further, the Principles define PII as data that, by themselves or in conjunction with other data held by a member, uniquely identifies an individual *offline*. Under the IAB Principles, tracking by behavioural advertisers using IP addresses as secondary identifiers of data subjects requires only opt out consent as long as it does not process PII.[45] The Principles also do not ensure transparency about profiling such as requiring data controllers to give meaningful information to consumers about profiles that relate to them. Nor do the Principles address the question of whether application of a group profile to individual data subjects creates personal data.

Other than referencing UK data protection law, the Principles do not address how the concept of sensitive personal data should be applied to consumer profiling. Nor do the Principles provide specific guidance on whether some profiling may be so unfair or discriminatory that it should be prevented and redressed, except to caution members that there may be valid privacy concerns about creating marketing segments for groups other than children under thirteen years of age. Instead, the Principles leave it to the discretion of members whether to do so, as guided by the over-riding objective of maintaining user trust. Thus the IAB Principles insufficiently restrain companies from creating other sensitive market segments for profiling purposes that may have significant privacy implications. For example, the industry codes do not restrict the creation of sensitive profiles that target vulnerable groups of consumers such as: teenagers who are 13-18 years old; consumers likely to be of certain racial or ethnic backgrounds; consumers likely to have particular illnesses, diseases or disabilities; or consumers who are likely to engage in compulsive gambling or to be attracted to pornography. In fact, the only privacy gap related to profiling that the IAB Principles partially closes concerns the need to address creation of sensitive marketing segments related to children and the gap is only closed to the extent that the Principles prohibit creating behavioural advertising segments intended for the sole purpose of targeting children under the age of 13.[46]

Overall, the IAB principles fail to provide essential transparency to consumers about consumer profiling. For example, the IAB Principles fail to ensure meaningful access to information about the consumer profiles that are used to generate targeted advertising. Being able to access information about individually applied profiles and associated market segments (group profiles) would enable consumers to understand the reasons they have received targeted advertising and avoid unfair manipulation by advertisers or discrimination. Legislative reform could correct the shortcomings in the IAB Principles and ensure adequate privacy and data protection for UK consumers as it relates to profiling. Through the process of revising the EU's Data Protection Directive, and requiring Member States to implement these revisions in their national laws, such legislative reform would set new minimum privacy protections above those provided by the IAB Principles.

3.2 The NAI's Self-Regulatory Code of Conduct. The NAI Code is a leading example of industry self-regulation by the behavioural advertising industry in the U.S.. As such, it reflects the relatively weak U.S. regulatory framework for information privacy that lacks generally applicable data protection and privacy legislation.[47] The NAI Code includes six basic fair information practice principles: 1) notice; 2) choice; 3) use/transfer limitation; 4) access; 5) reliability and 6) security.[48] Compliance with these six principles is not required by law in the U.S., however once a company makes a commitment to consumers that it will follow them, the FTC may enforce departures from the

[45] IAB Principles, note 37, Appendix 2 (Glossary, Personally identifiable information, Guidance Note 4, User Consent for OBA). See also, Poullet, note 3, p. 220 (discussing secondary identifiers that include IP addresses).
[46] IAB Principles, note 37, para. 3.3.
[47] The NAI is headquartered in the U.S. and many members who have promised to follow the NAI Code are located or operating in the United States. Website, NAI, York, Maine, U.S., at: http://www.networkadvertising.org/index.asp (last accessed,23 July 2010); NAI Code, note 38, p. 3 (Introduction) (commenting that the NAI worked with legislators [in the U.S.] and the FTC to develop the NAI Code). See also, NAI, Full Compliance Members, available at: http://www.networkadvertising.org/participating (last accessed,23 July 2010).
[48] NAI Code, note 38, pp. 7-10.

company's commitment as unfair or deceptive trade practices under Section 5 of the FTC Act.[49] The NAI Code broadly defines online behavioural advertising as any process used whereby data are collected across multiple web domains owned or operated by different entities to categorize likely consumer interest segments for use in advertising online. The Code applies to third-party OBA as well as to first party advertising and contextual advertising.[50] Under the NAI Code a member must provide robust notice on its website that is clear and conspicuous and includes six specified types of information.[51] The NAI code requires a level of consumer choice ranging from "opt out" to "opt in," with the level of choice being commensurate with the increased privacy implications of the data to be used.[52] Opt in consent is required to collect sensitive data (whether it is PII or not).[53]

Like the IAB Principles, the NAI Code fails to close the key privacy gaps that exist with regard to consumer profiling by behavioural advertisers. As in the IAB Code, the NAI Code's definition of PII does not include users' IP addresses or other secondary identifiers. Members who claim to be in compliance with the NAI Code frequently state in their policies that they collect and use non-PII, including users' IP addresses, and members' privacy policies still describe cookies placed on a unique browser as anonymous.[54] On the other hand, one of the significant fair information practices furthered by the NAI code is recognition that merging of PII with non-PII is deserving of being covered by requirements to obtain consumers' notice and consent.[55] The NAI Code expressly addresses the potential that advertisers may merge PII and non-PII, whether retroactively or prospectively, thus undermining consumers' initial consent and giving rise to enhanced privacy concerns for consumers. The merger of non-PII with PII is an important concern with consumer profiling because it may enable anonymous profiles to become identified with individuals. However, the NAI Code creates no obligation for members to provide access to information about

---

[49] FTC Act, 15 U.S.C. § 45 (Section 5).

[50] NAI, "NAI Response to Public Comments Received on the 2008 NAI Principles Draft," pp. 6-12, 16 December 2008 (clarifying that the NAI Code applies to Ad Delivery & Reporting (on a single website) and multi-site Reporting (across multiple websites, as well as traditional OBA) (NAI Response to Public Comments on 2008 NAI Principles Draft), available at: http://www.networkadvertising.org/networks/NAI%20Response%20to%20Public%20Comments_Final%20for%20Website.pdf (last accessed,23 July 2010) . Currently the NAI Code does not address the issue of behavioural targeting by ISPs. NAI Response to Public Comments on 2008 NAI Principles Draft , p. 8.

[51] NAI Code, note 38, p. 7 (requiring the following six forms of notice: 1. the OBA, Multi-site advertising and/or Ad Delivery & Reporting activities undertaken by the member company; 2. the types of data are collected by the member company; 3. how such data will be used by the member company, including transfer, if any, of data to a third party; 4. the types of PII and non-PII that will be merged by the member company, if any, and how any merged data will be used, including transfer to a third party; 5. an easy to use procedure for exercising choice to opt out or opt in with respect to such data use for OBA; and, 6. the approximate length of time that data used for OBA, multi-site advertising and/or ad delivery and reporting will be retained by the member company).

[52] PII is defined to include name, address, telephone number, email address, financial account number, government-issued identifier, and any other data used or intended to be used to identify, contact or precisely locate a person. Exhibit 1 (What type of notice is required for inclusion in OBA?).

[53] Sensitive data is defined to include social security numbers or other government-issued identifiers, insurance plan numbers, financial account numbers, information that describes the precise real-time geographic location of an individual and precise information about past, present, or potential future health or medical conditions or treatments, including genetic, genomic and family medical history. Exhibit 1.

[54] See, e.g., Complaint, Request for Investigation, Injunction and Other Relief: Google et al., Center for Digital Democracy (CDD), U.S. PIRG (a federation of state Public Interest Research Groups), World Privacy Forum (CDD et al.), before the Federal Trade Commission (FTC), p. 25 (8 Apr. 2010) (CDD Data Profiling Complaint), available at: http://democraticmedia.org/files/u1/20100407-FTCfiling.pdf (last accessed, 23 July 2010) (asking the FTC to investigate behavioural advertisers including Microsoft, Google and Yahoo and leading companies providing auctioning and data collection/targeting systems that support consumer profiling, for unfair and deceptive trade practices under Section 5 of the Federal Trade Commission Act).

[55] NAI Code, note 38, p. 8 (providing that "use of PII to be merged with non-PII on a going-forward basis for OBA purposes … shall require provision of a consumer opt out mechanism …" and "use of PII to be merged with previously collected non-PII for OBA purposes … shall require a consumer's opt in consent at the time such PII is collected online, or if collected off line, is first used online").

profiles that relate to consumers. In fact it does not even create an obligation for members to provide consumers with access to their PII, which is consistent with the general lack of laws requiring that U.S. data controllers provide consumers with access to their personal data.[56] Nor does the NAI Code provide guidance on whether applying a group profile to an individual consumer creates personal data.

The NAI Code does provide some guidance on what is sensitive data and requires opt in consent to collect sensitive data (whether it is PII or not). Differing from the IAB Principles, the NAI Code defines sensitive data to include "precise real-time geographic location of an individual" and recognizes that the "precise location of an individual (such as can be ascertained through GPS-enabled devices) may well be of great use to enable highly-personalized targeted advertising, particularly in the mobile marketing range."[57] In regard to the privacy gap concerning whether the creation and use of some profiles for market segmentation purposes may be so sensitive that heightened regulation is needed, the NAI Code prohibits the use of PII or non-PII to create an OBA segment specifically targeting children under the age of 13 without verifiable parental consent. It also specifies that OBA segments may only be used for marketing purposes, thus limiting secondary uses of marketing segments. However, the NAI Code does not impose limits on the creation or use of other sensitive marketing segments and does not limit assignment of consumers to those segments based on their profiles.[58] Nor does the NAI Code expressly restrict members from engaging in unfair or discriminatory profiling.

In the same ways that the IAB Code fails to provide transparency to consumers about profiling by behavioural advertisers, the NAI Code also fails. Nothing in the NAI Code requires members to give consumers access to meaningful information about the individual profiles that have been constructed about them or to disclose information to consumers about the group profiles to which consumers have been assigned. While the NAI Code requires behavioural advertisers to give notice of data collection at the point of collection or when anonymous data is merged with PII, and to provide consumers with at least the right to opt out of data collection, once data has been amassed by behavioural advertisers consistent with these obligations, transparency ends. Nothing in the NAI Code requires the advertiser to provide transparency related to the profiling processes that will be applied to the data, for example to disclose that the consumers' data in the advertisers' databases will be automatically data mined, that individual profiles will be produced (perhaps revealing "knowledge" about the consumer that the consumer himself or herself does not know), and that based on such profiles, individuals will be assigned to market segments/group profiles for marketing purposes. Thus, under the NAI Code, such processing for consumer profiling purposes may occur without regulatory protections to limit interference with consumers' personal autonomy and liberty and without regard to basic data protection principles such as transparency, proportionality or finality.

This article now considers how to close the privacy gaps that persist despite self-regulatory codes and currently available privacy-enhancing technologies.

4. The Need For Legislative Reform to Address Consumer Profiling

Privacy gaps in the current EU and U.S. regulatory frameworks leave consumers privacy and personal data unprotected in the context of profiling and behavioural advertising and industry self-regulatory codes and privacy-enhancing technologies do not close these gaps. Although revisions to industry codes and/or development of PETs and TETs could conceivably provide adequate protections for consumers' privacy and personal data in the

[56] There are exceptions to this general rule. For example, health care providers must give patients access to their personal health information, which is a form of personal data. See generally, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, in 42 U.S.C. § 1936 and other sections of the U.S. Code.

[57] Exhibit 1 (Is Sensitive data defined?); 2008 NAI Principles Draft, p. 11 (commenting that real-time geo-targeting data tracking points are deemed not only personal information, but also are further elevated to the status of sensitive customer information").

[58] NAI Response to Public Comments on 2008 NAI Principles Draft, note 50, pp. 20-24 (rejecting its draft proposal to require opt in consent for use of "restricted" or "sensitive" consumer segments in the final version of the NAI Code in favor of setting an "opt in" consent standard for use of any sensitive data for OBA, multi-site advertising or ad delivery & reporting uses, even if that data is not PII).

behavioural advertising context, currently this is not the case. The application of industry codes is limited to members of the the industry associations that have proposed them – each falls far short of establishing a national or global industry standard, fails to ensure fair information practices for consumer profiling and lacks adequate privacy enforcement mechanisms.[59] Further, adequate privacy-enhancing technologies are not currently available to empower consumers to protect their own privacy and personal data in the absence of government regulation mandating fair information practices.[60]

There is a need for government regulators in the EU and the U.S. to shape legislative solutions to protect consumers' privacy and personal data while establishing a consistent regulatory environment for the behavioural advertising industry's use of profiling, recognizing that targeted advertising promises benefits for both consumers and the industry, but consumers' also need adequate protections.. The Council of Europe's Draft Recommendation on Profiling (Draft Recommendation) and the U.S. Federal Trade Commission's Staff Report (FTC Guidelines) offer insights about how to adequately protect consumers in the context of profiling and behavioural advertising.[61] Each makes a strong contribution to this discussion with the Draft Recommendation offering broad privacy and data protection principles to address the general framework of profiling and the FTC Guidelines offering privacy and data protection principles for the specific context of behavioural advertising.

For mobile consumers to have an adequate level of privacy and personal data protection in the context of being profiled by behavioural advertisers, the six specific privacy gaps discussed earlier in this article need to be addressed. To close these gaps, this paper supports adoption of legislation to protect consumers' privacy and data protection applicable to profiling by behavioural advertisers. In this regard, it supports finalization of the Council of Europe's Draft Recommendation with revisions to address the shortcomings of the current draft as identified below and adoption of consistent Member State legislation. Further, it supports adoption of federal legislation in the U.S. to provide an adequate and equivalent level of protection for consumers in the context of profiling by behavioural advertisers.[62]

---

[59] See generally, Section 3 of this article and Exhibit 1. Lack of strong enforcement mechanisms has been recognized by industry groups that favor self-regulation, with announcement that industry self-regulatory groups will be launching a new system to police privacy abuses by companies that track consumers' web-surfing habits for ad targeting. See Steel, Emily, "To Stem privacy Abuses, Industry Groups Will Track Web Users," *The Wall Street Journal, WSJ.com* (24 June 2010). Reportedly, this effort of industry self-regulation is aimed at avoiding stricter federal regulation.

[60] Eckersley, note 23 (reporting on research showing that browser characteristics double as tracking tools); Simpson, J., 'Don't Google away your privacy rights,' *SFGate* (28 Jan. 2010) (arguing that consumers can't look to technology for lasting privacy protection because it is often too complex and cumbersome to use effectively; instead enforceable regulations are necessary based on broad principles rather than specific technologies), available at: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2010/01/27/ED3E1BOCHD.DTL (last accessed,23 July 2010).

[61] See Council of Europe, Draft Recommendation on the Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context of Profiling, The Consultative Committee of the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, T-PD-BUR (2009) 02 rev 5 Fin, p. 5 (resulting from the 21th Bureau Meeting, Lisbon, 13-15 April 2010) (CE Draft Recommendation on Profiling), available at: http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/events/t-pd_and_t-pd-bur_meetings/2T-PD-BUR_2009_02rev5_en_Fin.pdf (last accessed, 23 July 2010). See also, U.S. Federal Trade Commission's Staff Report (FTC Guidelines), note 39. The Council of Europe's Draft Recommendation and the U.S. Federal Trade Commission's Guidelines are analysed in the first article in this series. See *Profiling the Mobile Customer – Privacy concerns when behavioural advertisers target mobile phones, Part I, note 1*.

[62] See H.R. ___[Staff Discussion Draft], 111th Congress, lst Session, 'To require notice and consent of an individual prior to the collection and disclosure of certain personal information related to that individual,' (May 3, 2010) (The Boucher Bill), available at: http://www.boucher.house.gov/images/stories/Privacy_Draft_5-10.pdf (last accessed, 16 July 2010).This draft legislation was publicly released for comments from stakeholders and in all likelihood will be modified before it is formally introduced as proposed federal legislation. Guenwald, Juliana, 'Boucher Wants Bipartisan Privacy Bill,' *Tech Daily Dose, CongressDaily, National Journal* (10 June 2010). As of the date of this writing, The Boucher Bill has not yet been introduced into Congress. See also, H.R. 5777, 111th Congress, 2d Session, 'To foster transparency about the commercial use of personal information, provide consumers with

4.1 The need to restrict tracking consumers by their IP addresses and other secondary identifiers.

One of the most critical issues EU and U.S. regulators need to tackle with respect to behavioural advertising is whether the internet protocol (IP) address of an online computer user or a mobile user may be tracked without complying with fair information practices. For example, compliance with the fair information practices required by the Data Protection Directive is generally only required by those processing personal data and the question of whether IP addresses are personal data has not been definitively answered.[63]

It is important to recognize that IP addresses are a form of "secondary digital identifier," as compared to "primary digital identifiers" that are directly connected to the person, name, address, mobile phone number, passwords or electronic signatures.[64] "Secondary identifiers are indirect but are based on known information concerning the individual," such as unique identifiers stored in cookies, IP addresses or RFID tag numbers, and while they are "not necessarily known to the individual [data subject], are associated with a site or object with which the person is connected."[65]

Static IP addresses serve as constant identifiers, permitting individual's online behaviour to be tracked overtime and creation of individual profiles.[66] Also some IP addresses are dynamically assigned but include a static component ("hybrid" IP addresses). Like static IP addresses, hybrid IP addresses may enable identification of the user with some degree of accuracy and better support the creation of consumer profiles.[67] Further, even with assignment of a dynamic IP address that is not a hybrid IP address, it may be realistically possible to identify an individual user because other data is captured about the user's computer system or other personal data is available to enable identification and tracking of the user.[68] With regard to dynamically assigned IP addresses that are given to users

---

meaningful choice about the collection, use, and disclosure of such information, and for other purposes' (Rush Act of 2010), available at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h5777ih.txt.pdf (last accessed, 23 July 2010). The Rush Act of 2010 was introduced into Congress in July 2010, but, as of the date of this writing, has not yet become law. The various bills that are being discussed or drafted to protect consumers' online information privacy in the U.S. are still in their infancy and a thorough analysis of their provisions is beyond the scope of this paper.

[63] Data Protection Directive, note 43, art. 3(1). But see, Dinant et al., Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data: Application of Convention 108 to the Profiling Mechanism—Some Ideas for the Future Work of the Consultative Committee, T-PD(2008)01, Centre de Recherches Informatique et Droit (CRID), pp. 12-14, (Jan. 2008) (Dinant et al.), available at: http://www.statewatch.org/news/2008/aug/coe-profiling-paper.pdf.

[64] Poullet, note 3, p. 220.

[65] Ibid.

[66] IP addresses may be static or dynamic. Static IP addresses do not change and the same number is assigned to the same computer over time. Lah, F., 'Are IP Addresses "Personally Identifiable Information"?' 4 *I/S: A Journal of Law and Policy for the Information Society*, pp. 689-692 (2008-2009). In contrast, dynamic IP addresses are assigned to a computer for the duration of the user's Internet session and a new IP address number is assigned for each subsequent Internet use session. Ibid.

[67] Lah, note 66, pp. 689-691 (reporting that current IP addressing technology can contain a Host ID, or interface identifier, "that remains constant even when the Network ID, or topographic portion, of the address changes" and thus "may be considered a hybrid of the static and dynamic forms of IP addresses, with part of it remaining constant and the other part changing"). The "constant interface identifier could potentially be used to track the movement and usage of a particular device as it connects from different locations." Lah, pp. 689-691.

[68] Lah, note 66, pp. 692-704; Dinant, J. M., 'Chapter 5, The Concepts of Identity and Identifiability: Legal and Technical Deadlocks for Protecting Human Beings in the Information Society?' in *Reinventing Data Protection,* pp. 111-122 (S. Gutwirth et al. (eds.), Springer Netherlands, 2009) (commenting that dynamic IP addressing schemes offer little protection for consumers related to profiling). Dinant provides the example of Doubleclick, a company which systematically uses permanent unique identifying cookies and is present among various websites such that it is almost impossible to surf ten minutes on popular websites without opening transclusive hyperlinks (web bugs) to DoubleClick. Dinant, p. 116. As a consequence, DoubleClick is able to identify all the dynamic IP addresses used by

upon log-in, the EU's Article 29 Working Party concluded they are personal data when the log-in systems also record the date, time, duration of the user's access, and, using reasonable means, it is thereby possible to identify Internet users.[69] Under the Working Party's advisory opinion, both IP addresses and cookies that serve as unique user identifiers are personal data.

Because the behavioural advertising industry generally does not treat cookie data or IP addresses as PII unless they are otherwise associated with identifiable people, behavioural tracking of users by cookies or IP addresses may occur without adequate privacy protection in terms of fair information practices. For example, under the IAB Principles, the consumer tracked by his or her IP address would not be entitled to the fair information practices required by the Data Protection Directive when data about his or her online behaviour that is associated with that IP address is processed for profiling because the IAB Principles narrowly define PII as data that uniquely identifies an individual offline, thus excluding IP addresses and cookie data.[70] Further, the amended E-Privacy Directive's enhanced consent requirements for downloading or accessing most cookies on users' computers or mobile devices may not apply to cookies that do not collect any personal data.[71] For these reasons, if a mobile IP address (or other unique identifier associated with a particular mobile device such as a cookie) is not protected as personal data, the EU data protection framework will not restrain tracking by behavioural advertisers or require them to obtain advance consent before downloading cookies or accessing cookie data.

In contrast, the FTC Guidelines provide support for requiring fair information practices by behavioiural advertisers who track IP addresses or other secondary identifiers. According to the FTC, the FTC and other stakeholders "have long recognized that both PII and non-PII raise privacy issues" for five reasons:

- The possibility of merging non-PII with PII (such as merging tracking data with name and address);
- Development of new and more sophisticated technologies that may soon make it possible to link more IP addresses with specific individuals (including a new generation of IP addresses that makes this easier to do);
- The capacity for certain information that are anonymous by themselves to become identifiable when combined and linked by a common identifier;[72]

---

the same computer because those IP addresses have been sent together with a single unique identifying cookie. Dinant, p. 116 When considering whether reliance on dynamic IP addresses provides adequate privacy protection for consumers in the context of profiling, one should also consider that Google purchased DoubleClick in May 2007. Dinant, p. 116.

[69] Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data, pp. 16-17, 01248/07/EN/WP 136 (June 20, 2007) [hereinafter Art. 29 Opinion 4/2007], available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

[70] Exhibit 1 (What type of notice is required to use PII, definition of PII).

[71] See generally, Nauwelaerts, W., 'EU e-Privacy Directive and Cookies: The Consent Requirement May Not Be as Broad as Believed,' Hogan & Hartson (16 Nov. 2009) (Nauwelaerts, available at: http://www.hhdataprotection.com/2009/11/articles/international-compliance-inclu/eu-eprivacy-directive-and-cookies-the-consent-requirement-may-not-be-as-broad-as-believed/ (last accessed,23 July 2010). However, the Article 29 Data Protection Working Party recently provided its opinion that Article 5(3) of the amended E-Privacy Directive applies to placement and accessing cookie data even when personal data is not processed, clarifying that users' consent must be obtained prior to loading cookies or accessing data stored in those cookies even if the cookie or other information is not personal data. Article 29 Data Protection Working Party, Opinion 2/2010 on Online Behavioural Advertising, pp. 13-14 (00909/10/EN, WP 171, 22 June 2010) (Art. 29 Opinion 2/2010), available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp171_en.pdf (last accessed, 23 July 2010). Some of the behavioural advertising industry's leading participants disagree with this interpretation of Article 5(3). IABUK, 'Industry Unites to Reject Privacy Opinion' (25 June 2010), available at: http://www.iabuk.net/en/1/europeanmediaindustryunitesagainstarticle29opinion.mxs (last accessed, 23 July 2010). It is not yet known whether EU Member States will adopt the Article 29 Working Party's interpretation of Article 5(3).

[72] The FTC Guidelines provides the example of a consumer's internet activity that might reveal the restaurants in the neighborhood where she eats, the stores at which she shops, the property values of houses recently sold on her block and the medical conditions and prescription drugs she is researching. According to the FTC, the combination of this

- Recognition that the distinction between PII and non-PII may have no bearing on the sensitivity of the privacy risks at issue (for example, delivery of an ad associated with one user's searches on a computer may reveal sensitive private information to another user of the computer, even if the advertising does not reveal the identity of the user).
- Evidence that consumers are concerned about the collection of their data online regardless of whether the information is characterized as PII or non-PII.[73]

Accordingly, the FTC Guidelines include any data collected for online behavioural advertising that could reasonably be associated with a particular consumer or with a particular computer or device. This includes "clickstream data that, through reasonable efforts, could be combined with the consumer's website registration information; individual pieces of anonymous data combined into a profile sufficiently detailed that it could become identified with a particular person; and *behavioral profiles that, while not associated with a particular consumer, are stored and used to deliver personalized advertising and content to a particular device*."[74]

The FTC Guidelines demonstrate the right approach to resolve the privacy gap related to profiling enabled by IP addresses and other secondary identifiers. Whether static or dynamic, IP addresses should be treated as PII when reasonable means are available to permit user identification. However, mobile carriers often allow multiple Internet access customers to share a single IP address, making it more difficult to track mobile customers by their IP addresses.[75] While initially it would seem the mobile user has more privacy protection when accessing the Internet because not all access methods use IP addresses that facilitate individual profiling, the development of technologies that capture digital "fingerprints" of otherwise anonymous mobile devices accessing the Internet or that download persistent cookies to mobile devices enables websites to identify these users as well.[76] Accordingly, the privacy concerns that relate to tracking mobile users by their IP addresses also exist with development of digital fingerprinting technologies for mobile phones and tracking the use of persistent mobile cookies that serve to uniquely identify consumers.[77] The data produced by these new technologies should be treated as PII from a privacy

---

information would constitute a highly detailed and sensitive profile that is potentially traceable to the consumer. FTC Guidelines, note 39, p. 22.

[73] FTC Guidelines, note 39, pp. 22-23.

[74] FTC Guidelines, note 39, p. 26 (emphasis added). Of course the FTC Guidelines limit their applicability in other important respects, for example by excluding first party and contextual advertising from the definition of behavioural advertising and not including consumer access rights for either PII or non-PII data that is used for behavioural advertising purposes.

[75] Clayton, R., 'Practical mobile Internet access traceability,' Light Blue Touchpaper, Security Research, Computer Laboratory, University of Cambridge (13 Jan. 2010), available at: http://www.lightbluetouchpaper.org/2010/01/13/practical-mobile-internet-access-traceability/ (last accessed,23 July Apr. 2010).

[76] See Eckersley, note 23, p. 4 (discussing how device fingerprints are a "means to distinguish machines behind a single IP address, even if those machines block cookies entirely")last accessed,. Fingerprinting algorithms may be applied to databases of information captured when an Internet user's browser visits a website in order to produce a device fingerprint that can be used as a global identifier, akin to a cookie, to track the device. Eckersley, pp. 1-4. See also, 'Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Mobile Marketing Practices,' Center for Digital Democracy (to the Federal Trade Commission), pp. 23-28 (13 Jan. 2009) (describing mobile fingerprinting services for targeting web marketing that enable unique mobile user identification), available at: http://www.democraticmedia.org/current_projects/privacy/analysis/mobile_marketing (last accessed,23 July 2010). Currently certain browsers on mobile devices make them more difficult to fingerprint, however, these devices lack good cookie control options so they are readily trackable by other means such as mobile cookies. Eckersley, note 23, pp. 8-9.

[77] CDD Data Profiling Complaint, note 54, p. 26 (reporting that the behavioural advertising industry characterize cookies served to consumers as "unique number[s]" that are assigned to a consumer the first time an ad is served to him or her or identifies the consumer on a client's website).

perspective at least to the extent that they allow tracking of online and mobile devices and creation of individual consumer profiles.[78]

As discussed in the first article in this series, the regulatory framework in the U.S. does not give consumers basic privacy and data protection rights or mandate fair information practices by behavioural advertisers. So, whether or not an IP address or other secondary identifier is classified as personal data, it will not change this fundamental lack of consumer privacy and data protection under U.S. laws. Further, in the profiling context, the lack of privacy protections for consumers' mobile phone numbers is likely to result in privacy-intrusive tracking by behavioural advertisers in the U.S. Because the FTC Guidelines are not binding law they do not ensure fair information practices by behavioural advertisers. Thus new legislation is needed in the U.S. to protect the privacy and data of consumers profiled by behavioural advertisers. Additionally, the EU's Data Protection Directive and the Member State laws that implement this Directive need to be revised to address consumer profiling including tracking IP addresses and other secondary identifiers that can reasonably be associated with a particular consumer or a particular computer or mobile device.

4.2 The need to better define sensitive data.

One of the challenges for legislative reform to address consumer profiling will be to consistently define sensitive data. The definition of sensitive data in the resulting privacy laws will shape the content of consumer notices and the nature of requests for consent made by behavioural advertisers including whether advertisers must obtain opt in or opt out consent before collecting, using or sharing customers' data for profiling purposes. For consumers to give informed consent, they need to know the types of sensitive data that behavioural advertisers propose to process for profiling purposes. There is currently no consensus on what the definition of sensitive data should be in the context of profiling by behavioural advertisers.

The Draft Recommendation defines sensitive data consistent with the Data Protection Directive and essentially takes a human/civil rights approach, classifying personal data as sensitive if it identifies a consumer's race, political views, religious opinions, criminal convictions, or sex life. In contrast, the FTC Guidelines do not define sensitive data, instead providing "clear examples" of sensitive data. These examples include data that is sensitive under both a human/civil rights approach (e.g., data about children, health information) as well as an information privacy approach (e.g., financial data, location information and government issued Social Security numbers). To be adequate to protect consumers' privacy, an appropriate definition of sensitive data for behavioural advertising should consider both the human/civil rights approach and the information privacy approach. In this regard the Draft Recommendation's definition and the FTC's "clear examples" are both incomplete.

Examining the self-regulatory codes proposed by the behavioural advertising industry is also helpful in the search for an appropriate definition of sensitive data. The NAI Code provides the most precise definition. It defines sensitive data to include "social security numbers or other government-issued identifiers, insurance plan numbers, financial account numbers, information that describes the precise real-time geographic location of an individual and precise information about past, present, or potential future health or medical conditions or treatments, including genetic, genomic and family medical history."[79] However, this too is a deficient definition because it excludes data that is deserving of more privacy protection under a human/civil rights approach such as data about race, religion, and sex life. By way of comparison, protected classifications under U.S. civil rights laws differ slightly from the protected classifications under EU human rights laws, but a definition of sensitive data that comports with the civil rights approach from the U.S. would likely include data about a consumer's race, sex, age, national origin, religious beliefs or practices, and physical or mental disability. It would not, however, include political or criminal conviction data as is included in the Draft Recommendation's definition of sensitive data because discrimination based on these

[78] CDD Data Profiling Complaint, note 54, p. 25 (commenting that marketers claim that cookies and outside data attached to them are not personal data even though use of a cookie when combined with other offline data enables targeting by household).
[79] Exhibit 1 (Is sensitive data defined?).

categories is generally not prohibited under U.S. civil rights laws.[80] In contrast, the IAB Principles simply follow the Data Protection Directive's definition of sensitive data, which is also insufficient because this definition does not consider data that should be included under an information privacy approach.[81]

An appropriate definition of sensitive data should be included in EU and US legislation that will close this privacy gap related to consumer profiling by behavioural advertisers. Doing so will promote global consumer trust in the behavioural advertising industry that crosses geographical boundaries. This expanded definition should incorporate both a human/civil rights approach and an information privacy approach. It should specifically protect precise location data of mobile devices as sensitive data.[82] In identifying sensitive categories of personal data that should be protected by legislation, it would be helpful to resolve the differences between the Draft Recommendation and the FTC Guidelines such that a more comprehensive definition of sensitive data is established. Further, behavioural advertisers should be required to obtain opt in consent to process sensitive data for profiling purposes including collection and disclosure of location data related to mobile phones.

4.3 The need to regulate the creation and use of sensitive profiles.

As mentioned earlier, behavioural advertisers may apply data mining processes to databases of "anonymous" data about users' online behaviour and demographics. Through this individual profiles of consumers are produced that reference IP addresses or other secondary identifiers of consumers. Profiles associated with secondary identifiers such as IP addresses may allow advertisers to make inferences about sensitive data even though no actual PII or sensitive PII is used. Sensitive inferences may include the likelihood that the person using a particular IP address is of a certain age, race, national origin or sexual orientation, holds certain political beliefs or has a particular medical condition. Yet, under the Draft Recommendation, profiling by a behavioural advertiser that does not actually process personal data that is also sensitive data would not require the profiler to seek the explicit consent of the consumers profiled. While the FTC Guidelines recommend obtaining affirmative express consent from consumers before using sensitive data for behavioural advertising purposes, and both PII and non-PII may be sensitive data because these Guidelines do not make a distinction between PII and non-PII, the FTC Guidelines do not caution against or restrict advertisers from creating and using sensitive profiles.[83]

Leading industry self-regulatory codes do not sufficiently restrict the creation and use of sensitive profiles to protect consumers' privacy other than to prohibit profiling children under the age of thirteen.[84] The focus on protecting children under the age of 13 in both the NAI Code and the IAB Principles is consistent with the special status children generally have been given under the law. As the FTC says in its guidance about fair information practice principles:

---

[80] See, e.g., King, N., 'Fundamental Human Right Principle Inspires U.S. Data Privacy Law, But Protection Are Less Than Fundamental,' in *Challenges of Privacy and Data Protection Law* p. 42 (Cahiers Du Centre De Recherches Informatique Et Droit, 2008) (CRID treatise) (commenting that many questions that would be framed as human rights issues in the international arena are framed as civil rights issues in the US; civil rights focus on the ways in which states treat their own citizens while human rights exist in a broader international context that transcend a nation's laws); 42 Title VII of the Civil Rights Act of 1964, U.S.C. §§ 2000e to 2000e-17 (prohibiting employment discrimination on the basis of race, color, sex, national origin, and religion); The Americans with Disabilities Act, 49 U.S.C. §§ 12102-12118 (prohibiting discrimination on the basis of physical or mental disability);The Age Discrimination in Employment Act of 1967, 42 U.S.C. §§ 621-634 (prohibiting discrimination on the basis of age). These civil rights laws are not directly applicable to marketing practices that target consumers by protected classifications such as race, sex, etc. and there is a need to determine whether new legislation is needed to address unfair discrimination by behavioural advertisers that negatively impacts consumers due to membership in protected classifications.

[81] See Exhibit 1 (Is sensitive data defined?).

[82] Draft consumer information privacy legislation in the U.S. appropriately includes precise geo-location data in the definition of information and requires opt in consent for collection or disclosure of sensitive information. See The Boucher Bill, note 62, pp. 6-7.

[83] FTC Guidelines, note 39, p. 47.

[84] See Exhibit 1 (Is the creation of sensitive marketing segments limited?).

> "This status as a special, vulnerable group is premised on the belief that children lack analytical abilities and judgment of adults. It is evidenced by an array of federal and state laws that protect children, including those that ban sales of tobacco and alcohol to minors, prohibit child pornography, require parental consent for medical procedures, and make contracts with children voidable. In the specific arenas of marketing and privacy rights, moreover several federal statutes and regulations recognize both the need for heightened protections for children and the special role parents play in implementing these protections."[85]

Although members must commit to use of marketing segments only for marketing purposes, the NAI Code does not limit creation and use of marketing segments except as relates to children under thirteen.[86] Likewise, the IAB Principles allow individual members to exercise judgment about creating other marketing segments, although they expressly recognize that "there are valid privacy concerns about creating a segment for OBA in some areas because they could be considered sensitive in certain context" and there is a need for members to be guided by the "over-riding objective of maintaining user trust."[87]

In mobile commerce, sensitive consumer profiles created with access to mobile IP addresses and other secondary identifiers pose significant privacy concerns, even when there is no access to other personal data about the user. This is because a mobile IP address is increasingly likely to be a static address associated with a specific individual, as compared to IP addresses associated generally with computers that may have several users.[88] Further, although mobile carriers' use of geographic location (geolocation) information about mobile users generally requires obtaining users' advance consent in both the EU and the U.S., precise geolocation data can be collected by advertisers without using the services of mobile carriers or other highly regulated public communications services. For example, users may access the Internet using WiFi networks rather than carrier provided networks and mobile phones are being equipped with active RFID technology that can transmit information from mobile devices to other devices without using the carriers' services.[89] To illustrate the potential sensitivity of profiles about mobile customers, consider the creation of consumer profiles that include precise geolocation information about mobile users that is not covered by laws requiring behavioural advertisers to obtain consumers' advance consent for use of their location data. Such profiles could incorporate data associated with mobile IP addresses or other secondary identifiers indicating particular phones are near hospitals, bars, gambling casinos or red-light districts, etc. Yet, because mobile IP addresses and other secondary identifiers may not be considered personal data and/or sensitive data, the industry codes for behavioural advertisers and current EU and U.S. laws would not limit profiling of this nature. Only the NAI Code potentially would close this gap because it specifies that the "precise real-time geographic location of an individual" is sensitive data. But even the NAI Code does not address whether this type of data which is associated with a mobile IP address or a fingerprint of a mobile *device*, as opposed to an individual mobile user, is sensitive data.[90] This is a complex issue as the IAB Principles comment – one that should be discussed with wider stakeholders.[91] To the extent that regulation permits creation and use of sensitive profiles by behavioural advertisers, such regulation should require profilers to obtain opt in consent from those to be profiled and profiles utilizing geolocation information about mobile devices should be treated as sensitive profiles.

4.4 The need to give consumers access to information about individually applied profiles.

Consumers need access to relevant information about profiling processes used by behavioural advertisers and how profiling has been applied to them because this information is essential to exercising personal autonomy. Having

---

[85] 'Fair Information Practice Principles,' Federal Trade Commission, p. 3 (25 Jun. 2007) (citations omitted), available at: http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last accessed,23 July 2010),
[86] See Exhibit 1 (Is the creation of sensitive marketing segments limited?).
[87] IAB Principles, note 37, Guidance Note 5, Sensitive Segments.
[88] FTC Guidelines, note 39, p. 22 (footnote 50).
[89] 'Beyond Voice, Mapping the Mobile Marketplace,' FTC Staff Report, U.S. Federal Trade Commission, pp. 41-42 (April 2009), available at: http://www.ftc.gov/reports/mobilemarketplace/mobilemktgfinal.pdf (last accessed, 23 July 2010).
[90] See Exhibit 1 (Is the creation of sensitive marketing segments limited?).
[91] IAB Principles, note 37, Guidance Note 5, Sensitive Segments.

such notice and information enables consumers to be aware of possible manipulation by behavioural advertisers. As Heather Ng explains, "targeted ads can be highly manipulative, causing consumers to lose autonomy because of the ad companies' creation of psychological profiles based on the companies' perceived notions of the user's interest, rather than the user's own choices."[92] Ng argues that a person's personality development is impaired when that individual is not aware of being profiled and not able to learn what behavioural advertisers know about the person. Consumers' lack of knowledge about profiling hinders development of self-awareness and independent actions. The situation could be remedied by requiring advertisers to give consumers meaningful notice of profiling and access to the profiles that relate to them.[93]

The Draft Recommendation respects the personal autonomy of consumers by requiring profilers to give consumers notice of the profiling as well as certain types of information about the profiling.[94] By comparison, the FTC Guidelines and the NAI Code require notice to consumers of tracking for behavioural advertising purposes, but do not require disclosure to consumers of information about profiles applied to them.[95] The IAB's Principles do not directly require consumer access to information about profiles relating to them, although access would be required under the UK's data protection laws to the extent this information is determined to be personal data under the Data Protection Directive. Thus, the classification of IP addresses and other secondary identifiers as non-PII by behavioural advertisers (and under the currently ambiguous EU regulatory framework) becomes very important as it limits consumers' information access rights under the industry codes. Because profiles applied to mobile consumers are likely to be both more personalized (only one consumer usually uses a particular mobile phone) and more localized (may incorporate geolocation data about the mobile user), respect for personal autonomy is even more important for mobile users than for typical online consumers. Shouldn't the consumer know that she is receiving mobile coupons for a free hamburger at McDonald's restaurant because she used her mobile phone's web browser to check the movie listings for a theater near a McDonald's restaurant and her profile indicates she frequently visits fast food restaurants and buys weight-loss products?

Whether to mandate consumer access to information about individual profiles even when this information is non-PII is controversial because it may be difficult or expensive for behavioural advertisers to disclose meaningful information to consumers about the profiles that have been applied to them. Also, advertisers have historically been quite secretive about the market segments they use for advertising and may view disclosure of information about their profiling that assigns consumers to market segments as a revelation of proprietary market strategies that may undercut their competitive advantage in the industry.[96] The behavioural advertising industry may also argue it would be difficult to comply with this obligation because a consumer profile is essentially derivative information that is created by a computerized process that cannot be easily translated into understandable information for the consumer. But isn't that the point from a privacy perspective – to give the consumer useful information about how he has been profiled so that the consumer can correct any errors or simply alter his behaviour to avoid the consequences of future profiling? Being provided meaningful information about profiling by an advertiser is necessary for the consumer's exercise of his or her personal autonomy.

4.5 The need to protect consumers' ability to anonymously access information.

---

[92] Ng, note 11, p. 374.

[93] Profiling the European Citizen, note 28, p. 367 (according to Mireille Hildebrandt and Serge Gutwirth, "we will need transparency enhancing tools (TETs)" to "empower citizens to unfurl the profiling operations they are subject to"; "TETs, however, are still to be invented …."); Ng, note 11, p. 374.

[94] When profiles are "attributed to a data subject" new personal data may be generated that are not data that the data subject has communicated to the controller or that can reasonably be assumed by the data subject to be known to the controller., CE Draft Recommendation on Profiling, note 61, p.2 (para. 7). This Recommendation does not expressly state whether the data subject has a right to access individual profiles about himself or herself, although it does provide categories of minimum information about profiling that data subjects should be provided.. CE Draft Recommendation on Profiling, note 61, p. 7 (para. 5).

[95] See Exhibit 1 (Does the code offer consumers meaningful access to information about the profiles used to send them targeted advertising?).

[96] See Hotaling, A., "Protecting Personally Identifiable Information on the Internet: Notice and Consent in the Age of Behavioral Targeting," 16 *CommLaw Conspectus*, p. 537 (2008) (Hotaling).

Respect for personal autonomy may also require giving consumers the right to anonymously access information on the Internet using their mobile phones, including the right to search for and read information without disclosing their names or other personally identifying information or being tracked by advertisers.[97] Consumers should have this right of anonymity except when it is necessary for the service provider to know a consumer's identity in order to provide the service. The Draft Recommendation would require consumers be given the option to have access to goods or services without having to communicate personal data to the provider, unless providing the service makes it necessary to know the data subject's identity.[98] The industry codes and the FTC Guidelines do not provide or advocate anonymous access rights for consumers. Instead these sources presume access to information that is otherwise free may be conditioned on consumers giving their consent for advertisers to use their personal data or IP addresses and other secondary identifiers for behavioural advertising purposes.

Giving consumers the right to anonymously access information on the Internet and on their mobile phones would empower them to avoid the negative ramifications of being watched and mischaracterized through profiling without giving up access to information on the web or having to resort to other protective behaviour, such as providing false personal data or using a browser that hides identifying information about the consumer (e.g., hiding one's IP address or other unique identifier for a mobile device).[99] Protection of personal autonomy including anonymous access to information is a principle that should be reflected in privacy and data protection legislation and industry self-regulatory codes. If privacy-enhancing technologies such as web browsers become available that are designed to protect the user's identity and hide the user's IP address or other secondary identifiers, it may be necessary to adopt legislation to ensure that online and mobile users are able to use these browsers to access web content without being required to give their consent for profiling.

4.6 The need to prevent and redress unfair or discriminatory profiling.

Apart from prohibiting use of marketing segments targeting children under the age of thirteen, the industry codes do not address unfair or discriminatory profiling by behavioural advertisers.[100] Although both industry codes and the FTC Guidelines require compliance with existing laws, it is not clear how consumer protection laws and discrimination laws apply to profiling.[101]

It can be anticipated that consumers may experience unfair or discriminatory profiling due to mischaracterization that occurs through profiling processes that assign the consumer to unfavorable market segments. The Draft Recommendation recognizes the possibility that profiling may result in unfair treatment of the consumer by "unjustifiably depriving him/her from accessing certain goods and services, such as bank credit, insurance and online services."[102] This Recommendation also recognizes the possibility that "profiling techniques … can enable the generation of new sensitive data concerning an identified or identifiable person or 'groups' of people with the same characteristics" and "expose individuals to particularly high risks of discrimination and attacks on their personal rights and dignity."[103]

---

[97] Professor Daniel Solove discusses the importance of consumers feeling free to receive information anonymously, not just to share it. Solove, D., *The Digital Person*, p. 17 (New York University Press, 2004). Further, Professor Julie Cohen says "The freedom to read anonymously is just as much a part of our tradition, and choice of reading materials just as expressive of identity, as the right to use or withhold one's own name." Cohen, J., 'The Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace,' 28 *Connecticut Law Review,* p.1012 (1996).

[98] CE Draft Recommendation on Profiling, note 61, p. 7 (para. 4.7).

[99] For example, Ixquick.com is a private search engine that promises to delete all users' IP addresses within 48 hours of collection, at: www.ixquick.com (last accessed, 23 July 2010).

[100] See Exhibit 1 (Is the creation of sensitive marketing segments limited?).

[101] See, e.g., Exhibit 1 (Relationship of self-regulatory code to applicable laws and regulations).

[102], CE Draft Recommendation on Profiling, note 61, p. 3 (para. 11).

[103] CE Draft Recommendation on Profiling, note 61, p. 3 (para. 12).

There are many other situations where profilers may collect data about consumers that relates to classifications that historically have been protected from invidious discrimination, such as collecting data to use for behavioural advertising that reveals the race of a consumer. Further, consumers could be assigned to market segments based on inferences from their tracked behaviour that they are likely to be members of groups that historically have been protected from discrimination. For example, profiling could be used to assign a consumer to a market segment based on an inference from the consumer's behaviour that the consumer has a certain physical disability. Regular visitation to a website sponsored by an organisation that sells equipment for those with mobility impairments could be the type of behaviour that would give rise to this sort of inference.

Another type of unfairness that may result from profiling of this nature is unfavorable price discrimination. If a consumer does not receive advertising for special offers that other consumers receive, profiling may be the reason. It has been observed that "privacy appears to be declining largely in order to facilitate differential pricing" and there is a "growing incentive to price discriminate, coupled with the increasing ability to price discriminate."[104] For example, "adaptive pricing" enables online booksellers to change book prices "automatically depending on the demand of their clients, calculated by sophisticated formulas incorporating client profiles."[105] Whether this is or should be unlawful in the EU or in the U.S. and whether there is a need for legislative reform to address profiling that facilitates unfair price discrimination, is a question that is beyond the scope of this paper. However, these are questions that will likely need to be addressed as the behavioural advertising industry grows.[106]

Efforts to address the previously identified privacy gaps, particularly to define sensitive data, address the use of sensitive profiles and ensure protection of personal autonomy, would serve to minimize the risks to consumers of unfair or discriminatory treatment from profiling by behavioural advertisers. Beyond these concerns questions remain regarding whether there should be limits on the use of profiling for the purpose of engaging in price discrimination and whether privacy and data protection regulation should be used to address these types of issues rather than addressing them through contract, competition or other sources of law.

5. Conclusion

Legislative reform in both the EU and the U.S. is needed to protect consumers' privacy and personal data when behavioural advertisers use consumer profiling to target mobile users. Privacy-respecting industry self-regulation and privacy-enhancing technologies would also be helpful, but without legislative reform, they are not currently adequate to protect consumers' privacy and personal data in the framework of profiling that includes behavioural advertising.

At the present, neither EU nor U.S. laws adequately regulate consumer profiling for behavioural advertising purposes. Both regulatory systems leave consumers vulnerable to targeted advertising practices that invade their privacy and make unauthorized use of their personal data. While EU consumers have data protection rights regarding advertisers' use of their personal information and privacy is recognized as a fundamental right in the EU, it is not clear how these laws apply to consumer profiling or to behavioural advertising. Some of this uncertainty occurs because EU laws generally focus on personal data processing. This uncertainty could be remedied by legislation clarifying that data protection laws apply to consumer profiling for behavioural advertising purposes even

---

[104] Odlyzko, A., "Privacy, Economics, and Price Discrimination [Extended Abstract], Digital Technology Center, University of Minnesota, p.1 (2003), available at: http://www.dtc.umn.edu/~odlyzko/doc/privacy.economics.pdf (last accessed, 23 July 2010).

[105] Poullet, note 3, p. 212.

[106] Some scholarship already exists on this topic. See generally, Acquisti, Alessandro and Varian, 'Conditioning Prices on Purchase History," 24-3 *Marketing Science*, pp. 367-381 (2005) (examining when it is possible for sellers to condition their price offers on consumers' prior purchasing behaviour and whether it is profitable to engage in this form of price discrimination when consumers can adopt strategies to protect their privacy); Edwards, M., 'Price and Prejudice: The Case Against Consumer Equality in the Information Age,' 10 *Lewis and Clark Law Review*, p. 559 (2006) (positing that despite consumer antipathy, most forms of price discrimination are not unlawful under U.S. law when applied to end-use purchasers of consumer goods and services and demonstrating why the current state of affairs might reflect good public policy).

when the profiling is based on tracking users' IP addresses or other secondary identifiers in situations where it is reasonably possible to identify individual users. There is also no clear legal right for EU consumers to obtain meaningful information about the profiles that have been applied to them in order to generate targeted advertising. This situation is a failure of transparency from the consumer's perspective and an interference with the consumer's privacy in terms of personal autonomy.

In the EU, legislative reform is ongoing. The Council of Europe's Draft Recommendation is a first step towards legislative reform by its Members to apply data protection and privacy principles to consumer profiling. If finalized and adopted by Members of the Council of Europe, it will clarify the application of data protection to consumer profiling, establish consumers' rights to access information about the profiles that have been applied to them and give consumers a mechanism to object to unfair or discriminatory profiling. Additionally, when the revised E-Privacy Directive takes effect in the coming months, it will give consumers more control over whether they are tracked by cookies for behavioural advertising purposes. However, because not all such cookies may be covered by the amendments to the E-Privacy Directive, uncertainty on this issue may remain for both behavioural advertisers and consumers. The interpretation of the Article 29 Working Party that opt in consent is required to load tracking cookies onto consumers' phones and computers even when cookies do not collect personal data is certainly controversial. If this view is adopted by EU Member States, it may seriously impede the growth of the industry.

The behavioural advertising industry in the U.S. is even less regulated than in the EU and consumers have minimal data protection and privacy rights related to profiling and behavioural advertising under U.S. laws. In the U.S., there is no general regulatory framework for privacy and data protection and consumer privacy is not recognized as a fundamental right in the business to consumer context. No U.S. law requires behavioural advertisers to obtain consumers' consent before loading tracking cookies onto their computers, at least when spyware is not involved. Mobile customers do have some enhanced legal protection as mobile carriers are highly regulated in the U.S. Consequently, carriers are restricted in their disclosure and use of certain forms of their personal data, including mobile users' location data. However, the behavioural advertising industry, including intermediaries like Google, is not currently governed by industry-specific privacy and data protection legislation that would require advertisers to employ fair information practices regarding consumer profiling, so the industry is largely allowed to self-regulate. Although the FTC is continuing to monitor the advertising practices of the industry and has issued self-regulatory guidelines, it has yet to directly regulate the industry to protect consumers' privacy and personal data. Whilebills to regulate the behavioural advertising industry or consumer profiling have been drafted and one has already been introduced in Congress, none have yet been adopted. The recently filed FTC complaint challenging profiling by the behavioural advertising industry as unfair and deceptive provides important insight into the privacy and data protection concerns that new legislation should address.

If the industry self-regulatory codes analysed in this article were significantly revised to provide strong personal data and privacy protections for consumers related to profiling, this would go a long way toward establishing an industry standard to protect consumers' privacy and personal data in both the EU and the U.S. Adoption of privacy-enhancing technologies, such as browsers that put consumers in control of whether or not they can be tracked for behavioural advertising purposes, would also enhance consumer privacy. But legislative reform will still be needed in both the EU and the U.S. This is so because industry codes are only enforceable against members who agree to them, leaving many companies not committed to these codes. Effective privacy-enhancing technologies are not yet available.

The Council of Europe's Draft Recommendation is an important tool to start the discussion about what type of legislative reform is needed. While it is intended primarily for an EU audience, the Council of Europe recognizes the need for a global discussion of the important privacy and data protection concerns associated with customer profiling. This discussion should consider the specific contexts of profiling by behavioural advertisers and the heightened privacy and data protection concerns of mobile customers. It should also consider the need for global standards that will provide a consistent regulatory environment for consumer profiling by the behavioural advertising industry.

Authors' contact information:
Nancy J. King
Associate Professor
College of Business, Oregon State University
200 Bexell Hall,
Corvallis, OR 97331-2603, U.S.A.
E-mail: Nancy.King@bus.oregonstate.edu

Pernille Wegener Jessen
Associate Professor
Centre for International Business Law (CIBL)
Department of Business Law
Aarhus School of Business, Aarhus University
Hermodsvej 22, 8330 Åbyhøj, Denmark
E-mail: pwj@asb.dk

Nancy J. King's biographical information:
Nancy J. King is an Associate Professor at Oregon State University's College of Business in Corvallis, Oregon, U.S.A. In 2008 she was a Fulbright Fellow at the Centre de Recherches Informatique et Droit (CRID), University of Namur, Namur, Belgium. While at the CRID she conducted comparative legal research from an EU/U.S. regulatory perspective on data protection and privacy issues related to consumers' use of mobile phones incorporating location tracking technologies. She has published papers in the *International Journal of Private Law*, *Michigan Telecommunications and Technology Law Review* and the *Federal Communications Law Journal*, among others. She earned her Juris Doctor and Masters of Science in Taxation degrees from Gonzaga University, U.S.A. and her Bachelor's Degree in Accounting and Quantitative Methods from the University of Oregon, U.S.A. She is a Certified Information Privacy Professional. She currently teaches graduate and undergraduate business law courses at Oregon State University. She has served as a Visiting Professor at Aarhus School of Business in Aarhus, Denmark and Willamette University College of Law in Salem, Oregon. She was formerly an Associate General Counsel for a major U.S. corporation and a Partner with two law firms in Portland, Oregon.

Pernille Wegener Jessen's biographical information:
Pernille Wegener Jessen is an Associate Professor in EU law at the Centre for International Business Law, at the Department of Business Law, Aarhus School of Business, Aarhus University, Denmark. She is co-director of the research project *Legal Aspects of Mobile Commerce and Pervasive Computing: Privacy, Marketing, Contracting and Liability Issues* funded by the Danish Council for Independent Research; Social Sciences, and currently further participating in the research project: *WTO law and EU law: Integration and Conflicts* (also funded by the Danish Council for Independent Research; Social Sciences). She has published several books and contributions on issues related to EU competition and state aid law, and WTO law. She earned her Candidates Juris at Aarhus University and her Ph.D. degree at the Aarhus School of Business on the basis of a dissertation on EU state aid law. Since 2009 she has been a substitute of the Danish Competition Council. Currently she teaches graduate competition law courses at the Aarhus University.