Profiling the Mobile Customer – Privacy Concerns When Behavioural Advertisers Target Mobile Phones – Part I

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 – Privacy Concerns When Behavioural Advertisers Target Mobile Phones – Part I. *Computer Law and Security Review*, *26*(6), 595-612. doi:10.1016/j.clsr.2010.09.007

Profiling the Mobile Customer – Privacy Concerns 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 being tracked and profiled by behavioural advertisers to be able to send them personalized advertising. This process involves data mining consumer databases containing personally-identifying or anonymous data and it raises a host of important privacy concerns. This article, the first in a two part series on consumer information privacy issues on Profiling the Mobile Customer, addresses the questions: "What is profiling in the context of behavioural advertising?" and "How will consumer profiling impact the privacy of mobile customers?" The article examines the EU and U.S. regulatory frameworks for protecting privacy and personal data in regards to profiling by behavioural advertisers that targets mobile customers. It identifies potential harms to privacy and personal data related to profiling for behavioural advertising. It evaluates the extent to which the existing regulatory frameworks in the EU and the U.S. provide an adequate level of privacy protection and identifies key privacy gaps that the behavioural advertising industry and regulators will need to address to adequately protect mobile consumers from profiling by marketers. The upcoming second article in this series will discuss whether industry self-regulation or privacy-enhancing technologies will be adequate to address these privacy gaps and makes suggestions for principles to guide this process.[1]

Keywords: consumer profiling, data mining, online behavioural advertising, targeted marketing, mobile phones, mobile commerce, privacy, data protection.

1. Introduction

Behavioural advertising practices use profiling technologies to generate targeted advertising to consumers based on computer-generated profiles. Now that mobile phones increasingly include web browsing capability and location-tracking technologies, they are well designed for use by behavioural advertisers in order to produce highly-targeted advertising. Customer profiling by behavioural advertisers, and particularly profiling of mobile customers, raises important consumer privacy concerns that regulators in the European Union and the United States have yet to fully address.

This article is the first of a two part series on Profiling the Mobile Customer.[2] It begins with a discussion of the interplay among profiling, behavioural advertising and mobile customers' privacy. It identifies the potential harms that may arise from applications of consumer profiling for behavioural advertising purposes that should be addressed in order to adequately protect the privacy and personal data of mobile users. The article then outlines the regulatory

[1] 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.

[2] The second article in this two part series on Profiling the Mobile Customer will appear in the next volume of the CLSR. The second article looks at alternative approaches to protect consumer's privacy and data protection that include legislation, industry self-regulation and technology. It compares two leading self-regulatory codes from the United Kingdom and the United States that have been developed by industry associations for use by their members engaged in behavioural advertising. Concluding that there are serious deficiencies in these current self-regulatory approaches in terms of addressing key privacy and data protection concerns of profiling for mobile customers and that current technology is not adequate to protect consumers, it concludes that legislation needs to be adopted in both the EU and the U.S. to close the gaps in the current regulatory frameworks and support stronger industry self-regulation. It offers suggestions for that reform to both protect consumers and enhance the regulatory environment for mobile commerce.

frameworks in the European Union and United States that currently exist to protect consumer privacy and personal data in these two primary markets for global commerce. Current regulatory developments from Europe and the United States are discussed including an important draft recommendation on profiling from the Council of Europe, amendments to the E-Privacy Directive that further restrict placing tracking cookies on consumers' computers and self-regulatory guidelines for behavioural advertisers issued by the U.S. Federal Trade Commission. It identifies important privacy and data protection issues related to profiling mobile customers that are not addressed by the current regulatory frameworks but should be addressed by regulators to adequately protect consumers' privacy and personal data.

2. The Interplay Between Profiling, Behavioural Advertising and Mobile Customers' Privacy

One of the most challenging problems of living in today's information age is that "we are faced with an ever expanding mass of information" such that "*selection of the relevant bits of information* seems to become more important than the retrieval of data."[3] Profiling technologies promise a "technological means to create order in the chaos of proliferating data."[4]

Profiling is "an automatic data processing technique that consists of applying a 'profile' to an individual, namely in order to take decisions concerning him or her; or for analysing or predicting personal preferences, behaviours and attitudes."[5] In a technical sense, profiling is "a computerized method involving data mining from data warehouses, which makes it possible, or should make it possible, to place individuals, with a certain degree of probability, and hence with a certain induced error rate, in a particular category in order to take individual decisions relating to them." [6] This type of profiling "is similar to behavioral analysis since the aim is … to establish a strong mathematical correlation between certain characteristics that the individual shares with other "similar" individuals and a given behavior which one wishes to predict or influence."[7] Profiling "does not depend on human intelligence, but on statistical analysis of masses of figures relating to observations converted to digital form, [so] it can be practiced by means of a computer with minimum human intervention."[8]

Profiling is made possible by advances in computer technologies that involve the application of data mining to automatically search large databases of information about individuals' behaviour and demographics.[9] Profiling is accomplished by machines that run "software programs trained to recover unexpected correlations in masses of data aggregated in large databases."[10] Profiling does not merely query the database to find data that is already known to

---

[3] Hildebrandt, M. and Gutwirth, S. (eds.), *Profiling the European Citizen, Cross-Disciplinary Perspectives*, Springer, p.1 (2008) (Profiling the European Citizen) (emphasis in original).
[4] Ibid.
[5] 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.
[6] 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), p. 5, (Jan. 2008) (Dinant et al.), available at: http://www.statewatch.org/news/2008/aug/coe-profiling-paper.pdf .
[7] Ibid. (distinguishing consumer profiling by marketers from psychological profiling used by law enforcement to help identify criminal behaviour that attempts to get inside the criminal's mind).
[8] Ibid.
[9] Profiling the European Citizen, note 3, p.1.
[10] 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* 5 (2007), available at: http://www.fidis.net/fileadmin/journal/issues/1-2007/Profiling_into_the_future.pdf (alteration in original).

be there, such as the sum of attributes already recorded in the database, rather it attempts to "discover knowledge" that was not already known to be in the data.[11]

Essentially, behavioural advertisers use profiling technologies for direct marketing purposes – for example, websites that provide ad space for targeted advertising and/or network advertising companies often place tracking cookies on consumers' hard drives in order to gather data to construct consumer profiles for direct marketing purposes.[12] Direct marketers have long created market segments in an effort to create more relevant advertising and efficiently spend advertising dollars. What is new is advances in the tracking technologies that enable advertisers to construct personal profiles and use them to individually target consumers. Behavioural advertising (also referred to as behavioural targeting) "offers the highest return on investment for dollars spent on e-advertising – a value that is only diminished by the controversial nature of [behavioural tracking] technology."[13] Online behavioural advertising (OBA) applies automated data mining techniques to computer databases of information about consumer behaviour, such as digitally captured data about consumers' web surfing and online shopping activities and databases

---

[11] According to Hildebrandt:
Automated profiling can be described as the process of knowledge discovery in databases (KDD), of which data mining (DM; using mathematical techniques to detect relevant patterns), is a part. KDD is generally thought to consist of a number of steps:
(1) recording of data
(2) aggregation & tracking of data
(3) identification of patterns in data (DM)
(4) interpretation of outcome
(5) monitoring data to check the outcome (testing)
(6) applying the profiles.
Ibid. p. 5 (citations omitted). This type of profiling is new in two ways: it is produced by machines and it differs from classical empirical statistics because it results from a hypothesis that emerges in the process of data mining that is then tested on the population rather than a sample. Ibid. p. 6. An advantage of KDD is that it can "trace and track correlations in an ever-growing mass of retained data and confront us with inferences drawn from past behavior that would otherwise be lost to oblivion." Ibid. (citations omitted).

[12] Electronic Privacy Information Center (EPIC), Privacy and Computer Profiling (describing profiling practices related to direct marketing and listing numerous profile classifications that marketers may link to individual identities), available at: http://epic.org/privacy/profiling/ (last accessed 7 June 2010). Stakeholders benefiting from online advertising to include: "1) Providers: a. of targeted advertising (on site or on network) [and] b. of content and services which display ads against payment … [and] 2) Advertisers wishing to sell their products and boasting them through ads." Online targeted advertising, Cabinet Gelly, p. 6, available at: http://pg.droit.officelive.com/Documents/Online%20Targeted%20Advertising%20-%20CNIL%20Report%202009%20-%20Cabinet%20Gelly.pdf (CNIL Report, partial English translation) (providing a "partial, unofficial and uncertified [English] translation" of sections of the report presented by Mr. Peyrat, Commissioner, to the French Data Protection Authority (CNIL) on February 5, 2009 and released on March 26, 2009). The original French version of the CNIL Report is available at: http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/Publicite_Ciblee_rapport_VD (last accessed 27 May 2010) The CNIL Report includes description of the online behavioural advertising industry and analysis of legal issues raised by its practices under EU data protection law. It is the providers, rather than the purchasers of advertising, that generally collect data about website users that is used to build customer profiles. Ibid. Other important participants in the online behavioural advertising industry include associations of providers known as advertising networks. See Network Advertising Initiative, at: http://www.networkadvertising.org/participating/ (last accessed June 7, 2010) (providing a list of advertising networks that participate fully in the Network Advertising Initiative's self-regulatory Principles related to online privacy and the opt-out functions on this website). The term behavioural advertiser is used in this article to broadly refer to stakeholders in the behavioural advertising industry who are engaged in or benefit from consumer profiling for direct marketing purposes.

[13] See Hotaling, A., "Protecting Personally Identifiable Information on the Internet: Notice and Consent in the Age of Behavioral Targeting," 16 *CommLaw Conspectus*, p. 536 (2008) (Hotaling).

containing demographic information about potential customers.[14] This is done in order to produce highly-detailed knowledge profiles about customers that can be used to generate targeted advertising.

The creation and use of computer generated customer knowledge profiles enables businesses to provide highly individualized services and targeted advertising for their customers. The potential benefits of profiling for behavioural advertisers include improved market segmentation, better analysis of risks and fraud, and enhanced ability to adapt offers to meet demand.[15] Consumers also benefit from profiling that may enhance their user experience (e.g., when surfing the web using mobile devices), provide more relevant services and information (including online and m-advertising) and result in cheaper services, content and applications (because the cost is subsidized by advertising revenues).[16]

For online advertisers, application of profiling technologies offers the promise of individually tailoring advertising to consumers by using technology to shift through the mass of available data about consumers' interests, online and other behaviour and demographic data in order to discover information about consumers that can be used to generate more relevant advertising.[17] Behavioural advertisers have the ability to tailor their advertising messages for mobile users even more precisely than for other online customers by taking advantage of heightened ability to personalize and localize their marketing messages.[18] Because a mobile device is generally an individual communication device –

---

[14] Online behavioural advertisers use profiling for the purpose of customer relationship management (CRM) and specifically to produce individually targeted advertisements. Sophisticated machine profiling by businesses engaged in customer relationship management (CRM) is designed to gather "relevant data about as many (potential) customers as possible as part of marketing and sales strategies [in order to use that data to try to determine] which customers may be persuaded to become their new customers under what conditions." See Hildebrandt, note 10, p. 2. See also, Dinant et al., note 6, pp. 9–10 (discussing applications of data mining for personalized marketing and customer relationship management and marketing).

[15] CE Draft Recommendation on Profiling, note 5, p. 2 (para. 10); Hotaling, note 13, pp. 537-538 (explaining how online behavioural advertisers target consumers by acquiring user postings and clickstream data, analyse that data to form comprehensive personal profiles and serve advertisements that best match the interests expressed by the profiles). Hotaling also explains the direct marketing practice that segments tracked user history into distinct market segments. For example, within the broad market of automobiles, a company may create three distinct market segments: auto enthusiast, hybrid car shoppers and European import buyers. Ibid. p. 538. Then, based on a consumer's comprehensive personal profile, he or she would be assigned to one of these segments to be used for direct marketing purposes. Ibid. Behavioural advertisers are able to assign consumers to precise market segments (group profiles) based on individual customer profiles.

[16] Ibid.

[17] Benoist, E., 'Collecting Data for the Profiling of Web Users,' in *Profiling the European Citizen*, note 3, p. 172 (discussing applications of profiling that include implementation of one-to-one marketing that entails targeting information and special offers towards each specific client). Categories of data used by behavioural advertisers to produce targeted advertising include behavioural data (qualifies consumers based on interests), transactional data (transactions-based behavioural data based on conversations, etc., which may be real-time), and other demographic data (including data derived from user site registration, data verified at the household level, such as age, marital status, home-owner, etc). 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), pp. 11-13 (8 Apr. 2010) (CDD Profiling Complaint), available at: http://democraticmedia.org/files/u1/20100407-FTCfiling.pdf (last accessed, 7 June 2010).

[18] See Cleff, E., *Mobile Advertising: Proposals for Adequate Disclosure and Consent Mechanisms*, PhD Dissertation, Aarhus School of Business, Aarhus University, Aarhus, Denmark, pp. 30-31 (2009) (Cleff, Mobile Advertising Dissertation). Mobile commerce (m-commerce) includes all commercial transactions conducted through mobile communications networks that interface with mobile devices. Ibid. (citing Turban et al., *Electronic Commerce 2008: A Managerial Perspective*, p. 431 (Pearson Prentice Hall, 2008)). Mobile Advertising (m-advertising) is a part of mobile commerce. Cleff, Mobile Advertising Dissertation, p. 31. M-advertising can be defined "as the act of sending electronic advertisements to consumers who carry mobile devices." Ibid. p. 33. There are two major forms of m-advertising: "ads delivered in other media that feature a call-to-action, e.g., an m-

the mobile user is less likely to share his or her mobile device with other users – it is more personal than a desk-top computer (although the increasingly small size of portable computers may diminish this difference). Further, the behavioural advertiser may localize the advertising message to the mobile device's geographic location at a particular time, which is likely to be the same location as the user due to the personal and portable nature of the device.[19]

Services from third party data providers support real-time behavioural targeting by online advertisers to enable advertisers to reach specific users or to reject them as advertising campaigns are in progress (real-time behavioural advertising).[20] "Recent developments in online profiling and targeting—including the instantaneous sale and trading individual users … increasingly involve the compilation and use of greater amounts of personal data."[21] These developments include "a vast ecosystem of online advertising and data exchanges, demand- and supply-side platforms, and the increasing use of third-party data providers and online advertising and data auctions and exchanges that bring offline information to Internet profiling and targeting without the awareness or consent of users" (collectively "ad-exchange systems").[22] Initially developed in the U.S., ad-exchange systems are now being used in the United Kingdom and other parts of Europe and have moved to the mobile platform.[23]
Recent studies show consumers are concerned about their privacy and personal data in the context of behavioural advertising. They desire control over collection and use of personal information about them and they lack knowledge and understanding about data collection practices and policies.[24] One of the fastest growing consumer complaint categories in the U.S. relates to unauthorized creation of consumer profiles – a category that increased by 193% from 2007 to 2008.[25]

3. What are the Privacy Concerns for Consumers Related to Profiling and Online Behavioural Advertising?

The two primary privacy concerns for consumers being profiled for the purposes of behavioural advertising are interference with personal data protection and interference with personal autonomy and liberty.

3.1 Data Protection. When consumers access the Internet using computers, they leave behind a great deal of personal data about themselves including browsing behaviour and purchasing habits and demographic data such as their

---

advertising delivered via text messages, and ads delivered on the mobile device itself, e.g., within a mobile Web browser." Ibid. p. 34.
[19] Cleff, Mobile Advertising Dissertation, note 18, p. 34.
[20] See, e.g., CDD Profiling Complaint, note 17, pp. 4-5 (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). The Complaint asks the FTC to ensure consumers have meaningful control over their information and asks the FTC to seek injunctive and compensatory relief). See also, Press Release, CDD, U.S. PIRG, and World Privacy Forum Call on Federal Trade Commission to Investigate Data Collection 'Wild West' Involving Real-Time Advertising Auctions and Data Exchanges, *CommonDreams.org* (8 Apr. 2010), available at: http://www.commondreams.org/newswire/2010/04/08-0 (last accessed, 7 June 2010).
[21] CDD Profiling Complaint, note 17, p. 1 (para. 1).
[22] Ibid.
[23] Ibid. p. 28 (reporting that the Rubicon project serves both the UK and Europe and OpenX is working with Europe's largest ad network operated by Orange of France Telecom); Ibid. p. 20.
[24] Gomez et al., 'KnowPrivacy Report,' U.C. Berkeley School of Information, p. 5 (1 June 2009) (reporting the results of a recent study by graduate students comparing consumer expectations for online privacy with Internet companies' data collection practices, including how companies gather information about users' web activities using cookies and beacons, finding that despite consumer demand for control over how their personal information is collected and used, web analytics tools are used widely, often without users' knowledge), available at: http://knowprivacy.org/report/KnowPrivacy_Final_Report.pdf (last accessed 7 June 2010).
[25] Ibid. pp. 19-20 (reporting on data collected by TRUSTe about consumer complaints related to its member websites). See also 2009 Study: Consumer Attitudes About Behavioral Targeting, TRUSTe (4 March 2009), available at: http://www.truste.com/pdf/Behavioral_Targeting_Data_Sheet.pdf (last accessed 7 June 2010).

names, mailing addresses, phone numbers, etc. [26] Consumers generate even more personal data by using their mobile phones including geographic location data about the physical movement of their mobile devices from which inferences about the location of the owners of those devices may be made.[27] Mobile users also generate personal data related to their subscriptions with mobile carriers, such as billing information, types of mobile services received and calling history (phone numbers they have called or sent messages, the phone numbers of people who have called the subscriber or sent messages, the content of messages, etc.).[28] Mobile devices also store additional personal information, such as personal contacts, messages sent or received, photos, and other information.[29] Like other online users, when mobile customers use the web browsers in their mobile phones they communicate personal data that can be automatically collected and stored as personally-identifying or anonymous data in databases of carriers, advertisers or data warehouses.[30] These databases may also store data about mobile users that has been collected from other non-mobile sources including demographic data (e.g., name, address, phone number, income level, etc.) and behavioural data (e.g., web browsing behaviour from the users' home computers, purchasing activity in retail stores).[31] As described previously, databases containing consumer data can then be mined by automatic profiling systems designed to produce knowledge about consumers for targeted marketing purposes. Consumer profiling systems apply software to the data in the database to identify correlations between groups of consumers and produce group profiles for marketing purposes. Ultimately, a particular online or mobile consumer would be included in a group profile and the particular ads, promotions and other communications he or she receives would be based on this classification.

To the extent that profiling processes involve collection, use or disclosure of personally-identifying information (PII) about individuals, privacy concerns in the form of data protection arise. Potential consumer harms that arise from profiling consumers for behavioural advertising purposes include: 1) interference with consumers' rights of personal data protection (e.g., right to adequate notice and to give consent before their personal data is collected, used or shared for commercial purposes); 2) pervasive and non-transparent commercial observation of consumer behaviour (e.g., commercial tracking of mobile phone locations and surveillance of consumers' use of the Internet or mobile web browsers); 3) increased generation of unwanted commercial solicitations (e.g., online or mobile spam); 4) data security concerns (e.g., new exposures to risk of identity theft and fraud);[32] and 5) increased exposure to potential types of unfair commercial practices (e.g., offer or price discrimination between groups of consumers). These categories may overlap. For example, sending a location-targeted advertising message to a mobile user involves tracking the location of the consumer's mobile phone and processing personal data such as the user's

---

[26] See CE Draft Recommendation on Profiling, note 5, p. 2 (paras. 2, 3) (explaining that information and communication technologies (ICTs) allow the collection and processing of data on a large scale, including personal data, in both the private and public sectors, noting that continuous development of convergent technologies poses new challenges regarding collection and further processing of data). Data collection by ICTs may include traffic data and Internet user queries in search engines, data relating to consumer buying habits, data stemming from social networking and geo-location data concerning telecommunications devices, as well as the data stemming from video surveillance cameras, biometric systems and by Radio Frequency Identification Systems. Ibid.

[27] Ibid. Technology used for mobile communications brings together location and transaction information about users as well as personally identifiable information, creating a powerful new marketing tool enabling businesses to customize and personalize advertising for the mobile user. See Cleff, E.B., 'Implementing the Legal Criteria of Meaningful Consent in the Concept of Mobile Advertising,' 23-3 *Computer Law & Security Report*, pp. 262-269 (2007) (Cleff, CLSR).

[28] King, N., 'Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices,' 60-2 *Federal Communications Law Journal*, pp. 239-247 (2008) (King, FCLJ (2008)).

[29] Ibid.

[30] Ibid.

[31] Firms Merging Offline, Online Data to Improve Ad Targeting, International Association of Privacy Professionals (15 Mar. 2010), available at: https://www.privacyassociation.org/publications/2010_03_15_firms_merging_offline_online_data_to_improve_ad_targeting/ (last accessed 7 June 2010).

[32] Mantell, R., 'Identity theft is top consumer complaint,' *Market Watch* (14 Feb. 2008), http://www.marketwatch.com/story/identity-theft-is-no-1-consumer-fraud-complaint (last accessed 7 June 2010).

geographic location and mobile phone number. If the consumer hasn't consented to have his or her mobile phone's location tracked, the tracking is surveillance that interferes with the consumer's personal autonomy and private space. It is also spamming and an interference with the consumer's right to data protection if the consumer has not received notice and given consent to the advertiser to use the consumer's personal data (such as a mobile phone number) to send ads to the consumer's mobile phone.

The fact that consumer profiling can be conducted automatically by computers without being transparent to consumers undermines government regulatory efforts to legitimize the processing of PII by requiring businesses to employ fair information practices.[33] For example, a central element of fair information practices for the use of PII is to require processors to give consumers notice of the processing of their PII and to obtain their informed and voluntary consent to collect, use or share their personal data. But because consumer profiling may be pervasive, occurring nearly invisibly and continually in the background while consumers use the Internet and mobile devices and across multiple websites and databases, it makes it exceedingly difficult for processors to give consumers adequate notice and obtain consent and for consumers to effectively exercise their individual rights of notice and consent.[34]

3.2 Personal Autonomy and Liberty. To the extent profiling practices do not use personally identifying information about the individuals profiled, existing data protection laws may not apply.[35] Yet these business practices may still give rise to important consumer privacy concerns such as whether there should be limits on marketers' ability to use profiling if it interferes with the personal autonomy or liberty of consumers.[36] The use of profiling based on anonymous data to facilitate targeted marketing has been described as raising a privacy concern due to the resulting "asymmetry of access to knowledge" between customers and marketers.[37] The harm from this asymmetry of knowledge is that a customer who is "unaware of the profiles that are applied to her . . . may be induced to act in ways she would not have chosen otherwise."[38]

---

[33] See CE Draft Recommendation on Profiling, note 5, p. 2. When profiles are attributed to an individual consumer (data subject) it is possibleto generate new personal data. Ibid. The data subject has not communicated this new personal data to the controller and cannot be presumed to know about the new personal data generated by profiling, especially since the profiling activity may not be visible to the consumer. Ibid.

[34] Ibid.

[35] Use of anonymous data for profiling purposes may satisfy data protection rights under Council of Europe Convention 108 and the Data Protection Directive, but it does not eliminate the individual's privacy rights under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Dinant et al., note 6, pp. 30–31. See also, Article 15 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). However, when a profile is "attributed" to a data subject, at least arguably this attribution creates new personal data that the data subject did not communicate to the controller, and therefore the data subject's rights under the Data Protection Directive would apply. See CE Draft Recommendation on Profiling, note 5, p. 2 (para. 7).

[36] Scholars have argued that most profiling is done on the basis of anonymized data to which EU data protection legislation does not apply. See, e.g., Wim Schreurs et al., 'Legal Issues: Report on the Actual and Possible Profiling Techniques in the Field of Ambient Intelligence,' *FIDIS deliverable* 7.3, p. 49 (2005), available at: http://www.fidis.net/resources/deliverables/profiling/d73-report-on-actual-and-possible-profiling-techniques-in-the-field-of-ambient-intelligence/doc/26/ (last accessed 7 June 2010). In the same way, the application of a group profile to an anonymous person does not generally fall within the scope of EU data protection legislation, although it may have substantial consequences for this person. Ibid.

[37] Hildebrandt, note 10, p. 9. A second privacy concern is the risk of unfair discrimination based on refined profiling technologies that allow sophisticated market discrimination, such as price discrimination between groups of customers that is based on undisclosed group profiles. Ibid. p.10. While price discrimination "may be a good thing in a market economy . . . fairness again depends on consumers' awareness of the way they are categorized." Ibid.

[38] Ibid. p. 9.

Mireille Hildebrandt gives an example of a person whose online behaviour is profiled and matched with a group profile that predicts the chance that she is a smoker on the verge of quitting is 67 percent.[39] A second profile also predicts that if she is offered free cigarettes together with her online grocery purchase and receives news items about the reduction of dementia in the case of smoking, she has an 80 percent chance of not quitting.[40] If a tobacco company generates the profiles described above for marketing purposes, the customer's behaviour may be influenced, thereby inducing her to purchase cigarettes, yet she will be unaware of the group profiles used to target her as a potential customer by the marketer. From a privacy analysis, the customer cannot exercise her personal autonomy if she is unaware of the knowledge produced and used by the profiling practices of the marketer.[41] Protection of her privacy interest in this regard calls for providing a regulatory mechanism that will protect her autonomy by enabling her to gain access to the knowledge profiles that are used by marketers to select her for particular types of ads and promotions.[42] Presumably, if she has the same information as the marketers about the knowledge profiles she falls in, she may choose to exercise her autonomy and change her behaviour by resisting the free cigarettes or seeking treatment to stop-smoking. The important benefit of making the profiles transparent to the customer is that she is then empowered to acquire knowledge of the profiles enabling her to avoid being unfairly manipulated.[43]

In some cases, profiling may reveal customer profiles that describe characteristics of vulnerable groups of consumers who have historically been the subject of unfair discrimination. For example, profiling techniques may highlight correlations in otherwise anonymous data enabling the inference of sensitive data concerning identified or identifiable persons or groups of people with the same characteristics. Sensitive consumer profiles could include the probability that a consumer is of a certain race, holds particular political opinions, is a religious believer or nonbeliever or is heterosexual or homosexual.[44] One important question that needs to be resolved is whether application of a profile based on anonymous consumer data to an individual consumer creates personal data. At least arguably, when a profile is developed using anonymous data and that profile is applied to an individual consumer, it is made possible to generate new personal data.[45]

The use of automated customer profiling for direct marketing purposes may unfairly target vulnerable groups of consumers. Customer profiling may even result in depriving individuals in these groups of access to certain goods and services such as bank credit, insurance or online media services.[46] Examining some specific possible applications of consumer profiling for targeted advertising purposes to assess potential unfair or discriminatory impact on vulnerable groups raises serious questions about whether it may be necessary to limit some uses of

---

[39] Ibid. pp. 9–10.
[40] Ibid. p. 10.
[41] Ibid.
[42] Ibid. pp. 10–12, 15–17 (arguing for regulation that creates a privacy right to access, in real-time, knowledge profiles being applied to people; including the potential consequences, in order to protect personal autonomy). Hildebrandt argues that Transparency-Enhancing Technologies (TETs), as well as Privacy-Enhancing Technologies (PETs), need to be provided with respect to the use of the smart technologies that enable Ambient Intelligent (AmI) Environments). She lists sensor technologies, RFID systems, nanotechnology and miniaturization as the enabling technologies. Ibid. pp. 7, 15-17.
[43] See also, Ng, H., 'Targeting Bad Behavior: Why Federal Regulators Must Treat Online Behavioral Marketing as Spyware,' 31 *Hastings Communications and Entertainment Law Journal*, p. 374 (2009) (Ng) (commenting that "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").
[44] See CE Draft Recommendation on Profiling, note 5, p. 3 (para. 12) and p. 7(C.4.11) (recommending that the processing of sensitive data in the context of profiling be prohibited except if these data are necessary for the lawful and specific purposes of processing and domestic law provides appropriate safeguards). Sensitive data is defined to mean "personal data revealing the racial origin, political opinions or religious or other beliefs, as well as personal data on health, sex life or criminal convictions, as well as other data defined as sensitive by domestic legislation." Ibid. p. 5.
[45] See CE Draft Recommendation on Profiling, note 5, p. 2 (para. 7).
[46] Ibid.

consumer profiling by marketers. For example, should advertisers be able to use profiling to predict that a consumer will take advantage of a coupon for online gambling when the profile includes consumers who are likely to be compulsive gamblers? Is it acceptable for advertisers to use profiling to predict that a consumer will purchase weight-loss aids, when the profile includes consumers who are likely to be teenage girls with a very strong interest in looking thin? What if the weight-loss aids are promoted to consumers in a profile who have a high probability of having eating disorders, for whom weight loss aids may create substantial health risks? Should consumer profiling be restricted when it targets children or teenagers for marketing purposes, such as profiling to support ads aimed at children that encourage them to eat unhealthy foods high in fat and sugar, undermining the fight against obesity?[47] Is it permissible to use profiling to identify groups of consumers who are likely to have serious medical conditions, like cancer or diabetes, to target them for meditation and nutrition therapies? What about using profiling to identify groups of consumers likely to purchase products without doing price comparisons, when the profile focuses on consumers with lower educational accomplishments and income? Is it acceptable to target consumers in a profile that targets consumers with incomes below the poverty line for ads for legal, but high-interest, consumer loans? Given that consumers are unlikely to know the nature of profiles used to generate advertising offers to them under current behavioural advertising practices, consumers may be unfairly manipulated into making purchases by marketers without being empowered with the knowledge of why they are receiving the ads. Transparency is essential for consumers when marketers target consumers based on their probability of having addictions, illnesses, low income, youth, advanced age, lack of access to information, lower educational attainments or other factors that make groups of consumers vulnerable to unfair marketing practices and that are often beyond the control of individuals.[48]

Profiling of mobile customers makes it possible for advertisers to generate ads that are more personalized (individualized) and more localized (location-specific) as compared to traditional online behavioural advertising. Personalization is a distinguishing characteristic of profiling mobile customers because, generally speaking, mobile phones are personal devices that are typically used by only one person and so data associated with a particular phone is likely to pertain only to one user. In contrast, more than one user may use web access on a home computer on which a targeted ad is served. Localization is also a distinguishing feature of profiling mobile customers as GPS and other location tracking technologies produce location data that can be mined for profiling purposes and ads can be tailored for mobile users based on their precise geographic locations at particular times. These two distinguishing features of profiling mobile customers increase the risk for mobile consumers of being the subject of privacy-intrusive and/or unfair or discriminatory profiling practices for the purpose by advertisers. Further, advertisers' ability to deliver targeted ads on consumers' mobile phones only enhances the privacy concerns and other risks for mobile consumers.[49] For example, fast food ads based on profiling teenage customer behaviour and demographics can produce highly targeted ads to be sent to teenagers on their mobile phones. Such ads can be time and location targeted, arriving when teenagers are likely to be out of school and near fast food restaurants. This may make it more likely that teenagers receiving the ads will chose burgers and fries rather than healthy alternatives. Further, purchase of lottery tickets or the placement of wagers may be more likely to occur if consumers receive ads promoting these services on their mobile phones and are able to act immediately on the ads by entering nearby stores that sell lottery tickets or using the phones' web browsers to place online bets. In these situations, the profiling to support mobile ads for fast food or gambling likely targets only an individual mobile phone user, because a mobile phone is typically only used by one person rather than being shared. The enhanced personalization and localization

[47] Advertising and Consumer Rights, EurActiv.com (6 Jan. 2010) (reporting a recommendation by Ed May, chief executive of Consumer Focus, to place all children's websites under the supervision of the UK Advertising Standards Authority as an important step for children's rights because "At the heart of our request are recent research findings that UK children really do not understand that the company websites they use are designed as a marketing activity to build brand loyalty and to generate sales.") (Summary EU Advertising and Consumer Rights Regulation), available at: http://www.euractiv.com/en/innovation/advertising-consumer-rights/article-187133 (last accessed 7 June 2010).

[48] Ibid. (discussing the need to make allowances for vulnerable groups of consumers through regulation of advertising).

[49] The privacy implications of mobile marketing and regulation of mobile marketing practices have been explored in other articles and are generally outside the focus on consumer profiling in this article. See generally, King, FCLJ (2008), note 28 and Cleff, Dissertation, note 18.

that distinguishes mobile customer profiling means mobile customers need adequate privacy and data protection related to behavioural advertising.

4. Comparison of EU and U.S. Regulatory Frameworks for Behavioural Advertising and Mobile Commerce

Because the European Union and the United States are each others' largest trading partners, it is important to have compatible regulatory environments in each region to support the growth of global and mobile commerce.[50] Having compatible regulatory environments would provide stability for businesses operating across national boundaries and promote consumer trust.[51] Consumer trust is a significant factor leading to participation in e-commerce and creates an atmosphere where people are more willing to provide personal information. Consumer trust is influenced by consumers' expectations that their personal information will not be abused.[52] To a certain extent, the EU and U.S. regulatory environments are already consistent. For example, both the United States and the European Union generally prohibit abusive commercial practices including unfair or deceptive advertising practices.[53] These consumer protection laws help curb abusive marketing practices, including those of companies that adopt privacy policies as self-regulatory tools but then fail to live up to those policies.[54] Failure to protect the security of consumers' sensitive personally-identifying information is an unfair business practice in the U.S. and providing security for personal data is a requirement of the Data Protection Directive in the EU, even if the company has no

[50] Countries, U.S., European Commission Trade, available at: http://ec.europa.eu/trade/creating-opportunities/bilateral-relations/countries/united-states/index_en.htm (last accessed 7 June 2010).

[51] Villoch, A., 'Europe's Mobile Opportunity: Can the European Union Legislate Consumer Trust and Compete in the E-Commerce Market with the United States?' 20 *Pennsylvania State International Law Review*, pp. 446-48 (2002).

[52] Pavlou, P.A., 'Consumer acceptance of electronic commerce: Integrating Trust and Risk with the Technology Acceptance Model. 7(3) *International Journal of Electronic Commerce*, pp. 105-106 (2003) (defining trust in online retailing as "the belief that allows consumers to willingly become vulnerable to web retailers after having taken the retailer's characteristics into consideration"); Consumers' trust toward an online retailer is influenced by their perception of the likelihood that their personal information will not be abused. Rifon et al., 'Your Privacy is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures,' 39(2) *Journal of Consumer Affairs*, p. 345 (2005).

[53] Council Directive 2005/29/EC, OJ L 149/22, 11.06.2005 (Unfair Commercial Practices Directive) (last accessed 15 Jan. 2010); The Federal Trade Commission Act, 15 U.S.C. § 57a(a)(1)(b) (2010) (prohibiting unfair or deceptive trade practices). The European Union's Unfair Commercial Practices Directive, which must be implemented into Member-States' laws and allows Member-States to adopt national laws that provide additional health and safety protections for consumers, is similar to the Federal Trade Commission Act in the United States (FTC Act). Both EU and U.S. laws apply to unfair and deceptive marketing practices. Compare 15 U.S.C. § 57a(a)(1)(b) (2010) (providing FTC enforcement authority that covers unfair or deceptive acts or practices that occur in or affect interstate commerce) and the EU's Unfair Commercial Practices Directive, arts. 3, 11, 19. U.S. law also allows U.S. states to adopt laws that are more protective of consumers than the federal law. FTC, Comments of Verizon Wireless in re Telemarketing Sales Rules Review, FTC File No. P994414 (Fed. Trade Comm'n 16 May 2006), available at: http://www.ftc.gov/bcp/rulemaking/tsr/comments/verizon.htm (last accessed 7 June 2010). However, unlike the FTC Act, the EU's Unfair Commercial Practices Directive more specifically defines prohibited business practices. See, for example, see Unfair Commercial Practices Directive, arts. 6 (defining misleading actions), 7 (defining misleading omissions), 8 (defining aggressive commercial practices), 9 (prohibiting use of harassment, coercion and undue influence).

[54] For an example of a Federal Trade Commission enforcement action against a company that violated its own privacy policy, see Agreement Containing Consent Order, Gateway Learning Corp., File No. 042-3047 (Fed. Trade Comm'n 2003), available at: http://www.ftc.gov/os/caselist/0423047/040707agree0423047.pdf (last accessed 7 June 2010). See also, 15 U.S.C. § 57a(a)(1)(b); Unfair Commercial Practices Directive, note 53, art. 6(2)(b) (prohibiting, as a misleading action, the non-compliance with commitments made by a business that are capable of being verified (e.g., not merely aspirational) and made by a business in a code of conduct to which the business has agreed to be bound). The situation of businesses adopting privacy policies but failing to follow them is an example of the weakness in relying on industry self-regulation to protect consumers' privacy and personal data and why government regulation may be needed.

consumer privacy policy and the data is not sensitive.[55] Further, providers of mobile communications services (carriers) are heavily regulated in both the EU and the U.S.[56] Carriers are legally required to protect the privacy of subscribers' calling data and location data in both the EU and the U.S.[57] It is also true that online advertisers in both the EU and US have significant latitude to self-regulate as there is little legislation that restricts online advertising practices or content beyond general restriction on unfair or misleading advertising.[58]

However, as described in this section, the EU has a significantly more robust regulatory foundation for consumer privacy and data protection than the U.S. The EU's data protection regulation provides basic data protection rights for consumers in business to consumer advertising although it is unclear how these rights apply to the use of profiling for behavioural advertising purposes. Further, as analysed in this section, recent amendments to EU privacy laws that have not yet taken effect will provide enhanced protections for consumers in the context of the downloading of cookies onto users' terminal equipment, which is one of the key technologies that support delivery of behavioural advertising.[59] These amendments enhance the general foundation of EU consumer privacy

---

[55] See Eisenhauer, M., *The IAPP Information Privacy Case Book: A Global Survey of Privacy and Security Enforcement Actions With Recommendations for Reducing Risks*, International Association of Privacy Professionals (IAPP), pp. 53-55 (2008) (discussing the Federal Trade Commission's enforcement action in The BJ's Wholesale Club Case from September 2005 which concluded it is an unfair trade practice for a business to collect sensitive personal information, such as credit card numbers, unless reasonable security exists to protect the information). The EU's Data Protection Directive requires data controllers to provide security for personal data whether or not the data is sensitive. Data Protection Directive, note 35, art. 17.

[56] King, N., 'When Mobile Phones Are RFID-Equipped, Finding E.U.-U.S. Solutions to Protect Consumer Privacy and Facilitate Mobile Commerce,' 15 *Michigan Telecommunications and Technology Law Review*, pp. 156-168 (2008) (King, MTTLR (2008)). Under the European Union's regulatory framework, mobile phone devices and mobile communication services are regulated as information society services. See Thematic Portal, Information Society and Media Directorate, European Commission, at: http://ec.europa.eu/information_society/index_en.htm (last accessed 7 June 2010). Regulation of e-commerce is generally addressed as regulation of information society services. See, e.g., Directive of the European Parliament and of the Council 2000/31/EC of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular e-Commerce, in the Internal Market, OJ L 178/1,17.07.2000, preamble paras. 2, 4-5, 7-9 (E-Privacy Directive). The E-Commerce Directive requires that specified types of information be included in promotional offers and that required information be clear. Ibid. art. 6. Advertisements, including m-ads, must be identifiable to the consumer as commercial communications. Ibid. arts. 6(a), 7.

[57] King, MTTLR (2008), note 56, pp. 156-168.

[58] Summary EU Advertising and Consumer Rights Regulation, note 47, pp. 2-3 (commenting that "in principle, advertisers are bound by the code of conduct set out by the International Chamber of Commerce [ICC code of conduct], but electronic communications is outgrowing the current regulation and raising important questions regarding advertising and consumer rights in the online world."). See ICC International Code of Advertising Practice, Commission on Marketing, Advertising and Distribution (French Version, April 1997) (ICC code of conduct), available at: http://www.iccwbo.org/id905/index.html (last accessed 7 June 2010). In 2008 the Digital Marketing Communications Best Practice guidebook (October 2008) was produced by self-regulatory organisations that included advertising agencies (available at the website of the European Advertising Standards Alliance (EASA), www.easa-alliance.org) (last accessed 7 June 2010). Behavioural advertising was a particular concern raised in the European Commission's European Consumer Summit in 2009. On the topic of behavioural advertising, EU Consumer Affairs Commissioner Kuneva warned: "there is a lack of consumer awareness surrounding the collection of data," yet "personal data is the new oil of the Internet and the currency of the digital world." See Summary EU Advertising and Consumer Rights Regulation, note 47, p. 4.

[59] Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office; Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services; Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws; Directive 2009/140/EC of the European Parliament and of the Council of 25 November

protections and will impact the use of consumer profiling for behavioural advertising purposes. In contrast, the U.S. has not yet adopted similar legislation, although it has issued self-regulatory guidelines for behavioural advertisers and introduction of proposed federal privacy legislation to regulate the behavioural advertising industry is anticipated.[60]

4.1 EU Law. In the European Union, individuals have privacy and personal data protection under treaties and other legislation.[61] In addition to privacy rights articulated in the European Convention on Human Rights (ECHR), most Member States in the European Union have agreed to an international treaty on data protection known as Convention 108.[62] Two directives, the Data Protection Directive and the E-Privacy Directive are principal sources of applicable data protection legislation.[63] This body of privacy and data protection law as implemented through national laws largely establishes the rights of consumers and obligations of marketers that will govern behavioural advertising practices and profiling in the EU.

4.1.1 The Data Protection Directive (95/46/EC) requires EU Member States to adopt data protection legislation regulating the processing of personal data and the free movement of such data.[64] This Directive expressly refers to the fundamental rights of privacy that are contained in conventions and treaties. It states the intention to regulate the

---

2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services; 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities; and 2002/20/EC on the authorisation of electronic communications networks and services, OJ L 337, 18.12.09, pp. 1-69 (EU Telecoms Reform Package).

[60] 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 7 June 2010); Shields, M., 'Patrolling Bad Behavior, New FTC powers, Boucher Bill could crimp Web $,' *MediaWeek* (21 Mar. 2010) (reporting that U.S. Representative Rich Boucher is expected to introduce a new consumer privacy bill that will "impact the entire $25 billion online ad market and that the proposed financial reform bill would greatly expand the regulatory powers of the Federal Trade Commission). To date, draft legislation that would regulate the online behavioural advertising industry has been circulated for comment but has not yet been introduced into Congress. See Staff Discussion Draft, H.R. ____, A Bill to require notice and consent of an individual prior to the collection and disclosure of certain personal information relating to that individual, In the House of Representatives, 111th Congress, 1st Session (3 May 2010), available at: http://www.boucher.house.gov/images/stories/Privacy_Draft_5-10.pdf (last accessed 7 June 2010).

[61] See Treaty of Lisbon amending the Treaty on European Union, the Treaty establishing the European Community, OJ C 306/1, 17.12.2007 (recognizing Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and requiring Members of the European Union to respect the fundamental rights guaranteed by the Convention), consolidated version, available at: http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2008:115:SOM:EN:HTML (last accessed 7 June 2010). The Charter of Fundamental Rights of the European Union provides: "Everyone has the right to the protection of personal data concerning him or her." Charter of Fundamental Rights of the European Union, art. 8, 2000 OJ C 364/1 (hereinafter EU Charter), available at: http://www.europarl.europa.eu/charter/pdf/text_en.pdf (last accessed 7 June 2010).

[62] Ibid.; Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data including its additional protocol (CETS 108, 1981 and CETS 181, 2001, hereinafter convention 108); Polakiewicz, J, "'Smile! There's a camera behind the ad' or 'Send it to a friend': privacy in light of the new advertising techniques," 31st International Conference of Data Protection and Privacy Commissioners, Madrid, Spain (5 Nov. 2009) (explaining the application of the ECHR and convention 108 to automatic profiling practices including online behavioural advertising), available at: http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/Intervention%20Madrid%20Conference%205%20November%202009.pdf (last accessed 7 June 2010). See also, European Court of Justice, In re Bodil Lindqvist Case C-101/2001, recital 27, judgment 6 Nov. 2003 (holding the "act of referring, on an Internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes 'the processing of personal data wholly or partly by automatic means' within the meaning of Article 3(1) of Directive 95/46").

[63] See generally, Data Protection Directive, note 35; E-Privacy Directive, note 56.

[64] Data Protection Directive, note 35, art. 4.

processing of personal data consistent with these fundamental rights.[65] The Data Protection Directive generally applies only to the processing of personal data and limits its scope by defining personal data as information relating to an identified or identifiable natural person.[66] Under this Directive, individuals (data subjects) are assured certain rights with respect to their personal data while "data controllers" are required to follow rules and restrictions with respect to their data processing operations, including disclosing to data subjects the identity of any data controller and the purposes for which personal data are being collected.[67] The Data Protection Directive includes eight core principles of data privacy protection that define the rights of individual data subjects and the responsibilities of data controllers that process personal data, regardless of the context (consumer advertising, employment, etc.).[68] Pursuant to the Data Protection Directive, personal data may only be collected for specified, explicit and legitimate purposes and may not be processed inconsistently with those purposes (the "finality principle").[69] The purpose of the processing itself must be legitimate (legitimacy principle),[70] and the data subject must be fully informed on the details of the processing, including who has access to the data, how it is stored and how the subject can review it (transparency principle).[71] The "proportionality principle" requires that personal data be adequate, relevant and not excessive in relation to the purposes for which it is collected and further processed.[72] Sensitive data receives heightened data protection.[73] As a direct and mandatory result of the Data Protection Directive, there are national data protection laws in the EU Member-States that are administered by local data protection authorities and Member-States' data protection laws have been amended to be consistent with the Data Protection Directive's core principles.[74]

4.1.2. E-Privacy Directive. The E-Privacy Directive (2002/58/EC) was adopted to regulate the processing of personal data in the electronic communication sector. This sector includes publicly-available telecommunications

[65] Ibid. preamble para. 10 (providing that "the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law"). Privacy as a fundamental right is also recognized in international law. See, e.g., International Covenant on Civil and Political Rights and Optional Protocol to the International Covenant on Civil and Political Rights, G.A. Res. 2200 (XXI), U.N. GAOR, 21st Sess., Supp. No. 16, U.N. Doc. A/6316 (1966) (ICCPR).
[66] Data Protection Directive, note 35, art. 2(a) (including natural persons "who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"). But see Dinant et al., note 6, pp. 12–14 (stating that, unlike the other provisions in the Data Protection Directive, Article 15 of this directive, which deals with automated individual decisions, may make it unlawful to make a decision about an individual solely on the basis of automated data processing, even when no personally-identifying information is used in the process, if several cumulative conditions are met). The Data Protection Directive defines the processing of personal data broadly as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, . . . use, . . . dissemination, [etc]." Data Protection Directive, note 35, art. 2(b).
[67] Data Protection Directive, note 35, art. 10.
[68] The eight requirements to process personal data in the EU are: 1) fair and lawful processing; 2) collection and processing only for a proper purpose; 3) that data be adequate, relevant and not excessive; 4) that data be accurate and up to date; 5) that data be retained no longer than necessary; 6) that the data subject (consumer) have access to his or her data from the data controller; 7) that the data be kept secure; and 8) no transfer of personal data to a country that does not provide an adequate level of privacy and personal data protection. See generally, Data Protection Directive, note 35, arts. 6 et seq.
[69] Ibid. art. 6(1)(b).
[70] Ibid. art. 7.
[71] Ibid. art. 12.
[72] Ibid. art. 6(1)(c).
[73] Ibid. art. 8 (prohibiting the processing of special categories of personal data without explicit consent, with certain exceptions).
[74] See Data Protection Directive, note 35, p. 11; see also National Data Protection Commissioners, http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm (last accessed 7 June 2010).

and Internet services.[75] The E-Privacy Directive adopts the data protection principle of opt in notice and consent that requires advertisers to obtain users' consent prior to sending unsolicited advertising messages through publicly available electronic communications services.[76] There is one important exception to this rule: a person (natural or legal) is allowed to send electronic communications to a consumer in order to directly market the person's own similar products and services to the consumer.[77] Currently, consumers have an opt out right to refuse to have tracking software (such as cookies) or devices placed on their computers, mobile phones and other terminal equipment.[78] However, spyware, which by definition is deployed without users' knowledge or consent, is illegal if it is downloaded to a computer or mobile phone using a public carrier's network.[79]

In terms of data about telecommunications subscribers, the E-Privacy Directive defines traffic and location data of subscribers and is thus part of the regulatory framework for delivering location-based services.[80] Public carriers are prohibited from using traffic data for the purposes of marketing electronic communications services or for the provision of value-added services (e.g., location-based services including advertising and presumably in profiling processes utilizing traffic data to generate that advertising) without the consent of the subscriber to whom the data relates.[81] Additionally, unless location data has been made anonymous, public carriers must provide specific types of notice to subscribers and obtain their consent before processing location data (other than traffic data) to provide location-based services.[82]

---

[75] E-Privacy Directive, note 56, art. 1 (does not reflect 2009 amendments by the EU Telecoms Reform Package, note 59).

[76] E-Privacy Directive, note 56, art. 13(1). It specifically covers telemarketing calls made by autodialing equipment and electronic mail. Ibid.

[77] Ibid. art. 13(2). The exception only applies if all three of the following conditions are met: (1) the consumer is a customer of the person sending the direct marketing communications; (2) the consumer's electronic contact details were obtained by the person sending the direct marketing from the consumer in the context of a sale of a product or service; and (3) the consumer has the opportunity to object, free of charge, at the time the contact details were collected as well as later, to the sending of direct marketing communications. Ibid.

[78] The E-Privacy Directive prohibits using electronic communications networks to store information or to gain access to information stored in the terminal equipment of the subscriber or user unless consumers have been given clear and comprehensive information consistent with the Data Protection Directive and the opportunity to refuse processing of their personal data. Ibid. art. 5(3). Recent amendments to the E-Privacy Directive enhance consumers' privacy with respect to cookies but are not yet effective. See Section 5.1 of this article (the EU's Telecoms Reform Package).

[79] See *Concise European IT Law*, pp. 169-70 (Alfred Büllesbach et al. eds., 2006).

[80] Traffic data is "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof." E-Privacy Directive, note 56, art.2(b). Location data means "any data processed in an electronic communications network, including the geographic position of the terminal equipment of a user of a publicly available electronic communications service." Ibid. art. 2(c). The definition of location data has recently been amended broadening its scope as follows: "location data means any data processed in an electronic communications network *or by an electronic communications service*, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service." EU Telecoms Reform Package, note 59, at art. 2(c) (emphasis added to highlight the new wording). The scope of the E-Privacy Directive was also amended to clarify that it applies "to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices." EU Telecoms Reform Package, note 59, art. 3.

[81] Ibid. art. 6(3). Furthermore, the public carrier must erase or make anonymous such traffic data when it is no longer needed for the purpose of transmitting a communication, unless the subscriber has given consent or another exception applies. Ibid. art. 6(1).

[82] Ibid. art. 9(1). Article 9 also gives subscribers the right to withdraw their consent to the use of location data that is personal data. Ibid. art. 9(1)–(3). Location data: "May refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel; to the level of accuracy of the location information; to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time

4.1.3 EU Data Protection and Privacy Gaps. Recent analysis of the general strengths and weaknesses of the Data Protection Directive have been outlined in a comprehensive report sponsored by the EU Information Commissioner's Office (Rand Report).[83] One of the recommendations included in the Rand Report is to make European privacy regulation internationally viable for the future.[84] Achieving this recommendation will be critical to the development of a global regulatory environment that will support the growth of the mobile commerce and the behavioural advertising industry. Currently, the principles-based data protection framework gives consumers broad data protection and privacy rights and it is flexible enough to apply to all business to consumer contexts including profiling by behavioural advertisers. It is also technology neutral so it can be applied to different computer profiling technologies.[85]

Nevertheless the current data protection framework includes some regulatory gaps that create uncertainty when applied to behavioural advertising and profiling practices. First, it is not clear that consumers' IP addresses, which may be static (constant) or dynamic (change overtime from session to session), are personal data covered by the regulatory framework.[86] IP addresses are frequently tracked by behavioural advertisers to create consumer profiles. To the extent that behavioural advertisers do not associate cookies loaded on consumers' computers, their IP addresses or other secondary identifiers, and consumers' online or mobile behaviour with other personally-identifying data about consumers (such as their names), behavioural advertisers argue they are not processing personal data and the EU data protection framework does not apply to their marketing practices.[87] The EU's Article 29 Working Party considered the question of whether cookies and IP addresses are personal data and concluded that both IP addresses and cookies containing unique user identification are personal data.[88] The Working Party found

---

the location was recorded." Ibid. preamble para. 14. Access to location data is essential to providing location-based services through a telecommunications network.

[83] See also, Robinson et al., 'Review of the European Data Protection Directive,' Rand Europe, pp. 22-40 (Information Commissioner's Office, 2009) (Rand Report).

[84] Ibid. pp. 45-46.

[85] Rand Report, note 85, p. 24.

[86] 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. Static IP addresses serve as constant identifiers, permitting individual's online behaviour to be tracked overtime and creation of individual profiles. Ibid. A third form of IP addresses, sometimes called "hybrid" IP addresses, are dynamically assigned IP addresses that include a static component. Ibid. 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. Ibid. (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"). This type of "constant interface identifier could potentially be used to track the movement and usage of a particular device as it connects from different locations." Ibid. 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. Ibid. pp. 692-704.

[87] Data Protection Directive, note 35, art. 3(1); CNIL Report, partial English translation, note 12, pp. 10-11. See also, Dinant et al., note 6, pp. 12-14; Poullet, Y., 'Data protection legislation: What is at stake for our society and democracy?' 25 *Computer Law and Security Review*, pp. 220 (2009) (discussing secondary identifiers that include IP addresses).

[88] 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. Recently the Article 29 Data Protection Working Party sent a letter to three major search engines (Google, Yahoo! And Microsoft's Bing) warning them that their "methods of making users' search data anonymous," including retention of users' IP addresses for periods longer than necessary, were in conflict with the EU's rules on data protection. 'Internet search

dynamic IP addresses given to Internet users upon log-in by systems that also log in the date, time, duration of the user's access, can, using reasonable means, be used to identify Internet users and should be classified as personal data.[89] According to the Working Party, "unless the Internet Service Provider is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data, to be on the safe side."[90] The Working Party's opinion is advisory and it is not yet clear whether the Member States will follow it.[91]

The capacity to be tracked by IP address is a concern for mobile phone users who access the Internet by WLAN/WiFi (Wireless Local Access Networks) because such access uses IP addresses that can be used to construct individual profiles.[92] However, mobile carriers often allow multiple Internet access customers to share a single IP address, making it more difficult for mobile customers to be associated with a particular IP address.[93] While it would seem the mobile user has more privacy protection when accessing the Internet because not all access methods require revealing an individual IP address, the development of technologies that capture digital "fingerprints" of otherwise anonymous mobile devices accessing the Internet and the ability to download persistent cookies to mobile devices enables behavioural advertisers to identify these users as well.[94] Accordingly, the privacy concerns that

---

engines scolded by EU regulators,' EurActiv (27 May 2010), available at: http://www.euractiv.com/en/infosociety/internet-search-engines-scolded-eu-regulators-news-494549?utm_source=EurActiv+Newsletter&utm_campaign=2bbe971f0e-my_google_analytics_key&utm_medium=email (last accessed 7 June 2010). Search engine data is an important source of tracking data for behavioural advertising.

[89] Ibid.

[90] Art 29 Opinion 4/2007, p. 17.

[91] A German association of data protection authorities has ruled that tracking using IP addresses breaches German law. See 'Germany rules IP address tracking reaches data protection law,' *Napier News* (9 Feb. 2010), available at: http://www.napiernews.eu/2010/02/germany-rules-ip-address-tracking-breaches-data-protection-law/ (last accessed, 7 June. 2010). In contrast, A French Court held an IP address was not personal data. See 'IP Address in Anti-Piracy Probe Was Not Personal Data, Says French Court,' Out-Law.com (2 Feb. 2010), available at: http://www.out-law.com//default.aspx?page=10802 (last accessed 7 June 2010). The court's opinion is reported in French at: http://www.legalis.net/jurisprudence-decision.php3?id_article=2852 (last accessed 7 June 2010). Further, a decision by the European Court of Justice supports the view that IP addresses are personal data. See 'Online Behavioral Advertising, What All Global Companies Need to Know,' Baker & McKenzie (materials provided for a seminar on this topic held on 18 May 2010, referencing *Promusicae v. Telefonica*, a decision of the European Court of Justice, 29 Jan. 2008).

[92] Sarajlic, A. and Omerasevic, D., 'Access Channels in m-Commerce Services,' Proceedings of the ITI 2007 29th Int. Conf. on Information Technology Interfaces, Cavtat, Croatia, pp. 507-512 (June 25-28, 2007)(describing access channels for mobile users to m-commerce including those in the mobile operator network, WAP (Wireless Application Profile) and WLAN/WiFi (Wireless Local Access Networks). On the other hand, mobile users who access the Internet from a mobile phone using a cellular provider's data service or using WAP (Wireless Application Protocol) generally do not reveal their individual IP addresses. Ibid.

[93] Clayton, R., 'Practical mobile Internet access traceability,' Light Blue Touchpaper, Security Resaerch, Computer Laboratory, University of Cambridge (13 Jan. 2010), available at: http://www.lightbluetouchpaper.org/2010/01/13/practical-mobile-internet-access-traceability/ (last accessed 7 une 2010).

[94] Eckersley, P., 'How Unique is Your Web Browser?' Electronic Frontier Foundation (undated) (discussing that device fingerprints are a "means to distinguish machines behind a single IP address, even if those machines block cookies entirely"). 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. Ibid. pp. 1-4. See also, Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Mobile Marketing Practices, Center for Digital Democracy and U.S. Public Interest Research Group, 13 January 2009 (CDD Complaint of Unfair or Deceptive Mobile Marketing Practices) (amending November 2006 petition to the FTC requesting an investigation into and relief from tracking and targeting practices in online advertising), available at: http://www.democraticmedia.org/current_projects/privacy/analysis/mobile_marketing (last accessed, 7 June 2010).

relate to tracking mobile users by IP addresses also exist with development of secondary identifiers such as digital fingerprinting technologies and persistent cookies for cell phone tracking. The data produced by these technologies should be treated as personal data from a privacy perspective because they allow tracking of consumers' mobile devices and creation of individual consumer profiles.

Second, important questions for consumers include whether they are entitled to access meaningful information about the profiles that have been applied to them. Currently "profiles have no clear legal status," so it is not clear that data protection law applies to individually-applied profiles, relevant group profiles, relationships between group profiles or the way that these profiles are generated.[95] Legal protection against, or at least access to profiles is very limited. In data protection legislation there are two arguments supporting access to profiles by data subjects.[96] First, once a profile has been applied to an individual person, it becomes personal data for example, in the case of credit scoring practices. This answer, however, does not address the relevant group profile, its relation to other group profiles, or information about the way the profile was generated (by use of which algorithm etc.). Second, arguably, the autonomic application of profiles falls within the scope of Article 15 of the Data Protection Directive which limits automated decision making even if personal data is not used.[97] Art. 15 of the Data Protection Directive reads: "Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him."[98]

Third, it is not clear that individually-applied profiles created by behavioural advertisers are personal data because such profiles may be generated without using any personal data, at least to the extent that IP addresses and cookies are not personal data. This uncertainty exists because the EU's data protection framework currently does not apply to processing of data that is not personal data, although arguments may be made that consumers also have data protection from automated decisions that have legal effects on them and consumers' fundamental rights to privacy may apply in this context.[99]

Fourth, it is not clear how the Data Protection Directive's restrictions on using sensitive personal data should be applied in the profiling context.[100] There are significant differences in the global perspective on what is sensitive data. For example, the EU categories of sensitive data under the Data Protection Directive focus on data that is sensitive from a human rights perspective to include personal data that reveals racial origin, political opinions or religious or other beliefs as well as personal data on health or sex life.[101] In contrast, the U.S. Federal Trade Commission focuses on protecting financially sensitive data, such as consumers' credit card numbers.[102]

Currently certain browsers on mobile devices make them more difficult to fingerprint, however these devices lack good cookie control options so they are readily tracked by other means such as mobile cookies. Eckersley, p. 9.

[95] Hildebrant, note 10, p. 13 (arguing profiles "may be protected from access via intellectual property rights of the profiler or be considered part of the company's trade secrets).

[96] Ibid.

[97] Ibid.

[98] Data Protection Directive, note 35 (art. 15).

[99] Hildebrant, note 10, p. 13. See also, Rand Report, note 85, p. 27 (Information Commissioner's Office, 2009) (pointing out that one of the main weaknesses in the Data Protection Directive is that the link between the concept of personal data and real privacy risks is unclear).

[100] Compare CE Draft Recommendation on Profiling, note 5, p. 5 and FTC Guidelines, note 60, p. 42

[101] Data Protection Directive, note 35 (art. 8) (prohibiting the processing of special categories of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life unless the data subject has given their explicit consent or there are other legitimate grounds for processing the data).

[102] I*n the Matter of* BJ's Wholesale Club, Inc., Federal Trade Commission, FTC File No. 042 3160 (Sept. 2005) (finding the company's failure to adequately secure sensitive credit card information including customers' credit card numbers was an unfair practice under Section 5 of the FTC Act).

Fifth, it is unclear whether the creation and use of certain profiles for market segmentation purposes may be so sensitive that they should be more strictly regulated or prohibited even if no personal data is used in the process.[103] As discussed earlier in this article, customer profiling may create marketing segments related to children, health conditions and other potentially sensitive categories that deserve heightened regulation to prevent potential abuses from a privacy perspective.

Finally, it is not clear whether applications of profiling by behavioural advertisers may result in unfairness or discrimination against individual consumers even if no personal data is used in the process, such profiling that infers the consumer is in a market segment defined by low income, gender or race, that may need to be regulated and redressed.[104] This list of questions reveals privacy gaps in the current EU regulatory system that need to be answered in order to assess whether consumers have adequate protections for their privacy and personal data when profiling is used by behavioural advertisers.[105]

4.2. U.S. Law. U.S. law has long recognized privacy as a general notion and as an individual right. U.S. scholars have been instrumental in developing arguments that personhood, or the right to define one's self, is a core privacy value to be protected by law.[106] This conception of privacy protects the liberty and autonomy of natural persons although information privacy in the business to consumer context has not been recognized as a fundamental right in the U.S. and consumers receive less privacy protection from commercial intrusions into their privacy than they do from governmental intrusions.[107] Four distinct privacy torts are recognized by the courts in most U.S. jurisdictions giving an individual the right to bring a lawsuit to recover damages from one who unreasonably intrudes upon that person's seclusion whether physically or electronically, although the torts have proved ineffective as a general tool to protect individuals' information privacy.[108] No federal statute of general application comprehensively regulates businesses to protect consumers' privacy or data protection[109] and no federal laws have yet been adopted to specifically regulate behavioural advertising practices or automated profiling.[110] State statutes are also a potential

---

[103] CE Draft Recommendation on Profiling, note 5, p. 3.
[104] Ibid.
[105] These privacy gaps are further addressed in the second article in this series on Profiling the Mobile Customer that will appear in the next volume of the *CLSR*.
[106] Warren, Samuel and Brandeis, Louis, 'The Right to Privacy,' 4 *Harvard Law Review*, pp. 193-195 (1890) (arguing individuals have a "right to be let alone"); 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. 76 (Cahiers Du Centre De Recherches Informatique Et Droit, 2008) (CRID treatise) (discussing the evolution of privacy law in the U.S. and concluding U.S. privacy law falls short of protections data privacy as a fundamental human right).
[107] See generally, CRID Treatise, note 106, pp. 85-87, 97-98. As the U.S. Supreme Court said, "choices central to personal dignity and autonomy are central to the liberty protected by the Fourteenth Amendment [of the U.S. Constitution]. At the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe and of the mystery of human life." Ibid. p. 85 (quoting Planned Parenthood of So. Pa v. Casey, 505 U.S. 833, 851 (U.S. S. Ct., 1992).
[108] Solove, Daniel J., Rotenberg, Marc and Schwartz, Paul, *Information Privacy Law*, pp. 76-102 (2nd ed., 2006) (Solove et al.) (discussing numerous court opinions considering tort claims of intrusion into seclusion including wiretapping and other forms of electronic surveillance). To prevail in such a tort case the plaintiff must show both the unreasonable intrusion by the defendant and that the intrusion would be highly offensive to a reasonable person, but need not prove that the defendant publicly disclosed private information. Ibid, p.76; CRID Treatise, note 106, pp. 90-92.
[109] Ciocchetti, Corey, 'Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifying Information,' 10 *Vanderbilt Journal of Entertainment and Technology Law*, p. 609 (2008) (describing U.S. federal privacy law as "sectoral, protecting only certain individuals in certain economic sectors against certain privacy-invading threats") (Ciocchetti (2008). By comparison, The Privacy Act of 1974, 5 U.S.C. §552(a), is a law of general application that protects the personal information of individuals in their records that are maintained by government, however it does not regulate private businesses' collection or use of consumers' personal information.
[110] Beginning in 2008, Congressional subcommittees have been holding hearings to explore whether there is a need to regulate behavioural advertising, but no legislation has been adopted as of the date of this writing. Schatz, Amy,

source of consumer privacy and data protection law in the U.S. and may provide higher levels of protection than provided by federal law, except where preempted by federal law.[111] Although at least three states have proposed legislation regulating behavioural advertising, such legislation has not yet been adopted in any state.[112] This does not mean that behavioural advertising may not violate industry-specific data protection laws or laws that make using certain marketing practices unlawful, as next described.

4.2.1 Data protection laws. A patchwork of industry-specific, federal data protection laws have been adopted in the U.S. These laws, together with the Federal Trade Commission's (FTC) general enforcement powers, comprise the federal privacy and data protection framework. For example, federal statutes set minimum privacy requirements for: 1) websites that collect the personal information of children under the age of 13 years;[113] 2) financial institutions that collect personal information about their customers and consumers;[114] 3) health care providers that collect personal health information;[115] and 4) credit reporting agencies that collect information about consumers' credit histories.[116] Because profiling mobile customers may mine consumer data and behaviour related to use of telecommunications networks, laws regulating telecommunications carriers are also an important part of the federal regulatory foundation that relates to the use of behavioural advertising and mobile commerce. Telecommunication carriers are heavily regulated by the Federal Communications Commission (FCC) [117] and are required to provide privacy protection for subscribers' "customer proprietary network information" (CPNI).[118] CPNI includes sensitive data about a customer's telephone service such as who the customer called and the geographic location of the caller. However, the definition does not include the customer's mobile phone number or the type of personal information that would normally be included in a telephone directory, such as the subscriber's name or address.[119] Consequently, mobile phone numbers and other subscriber information that is not CPNI receive little or no privacy protection.[120] Further, CPNI regulation only applies to regulated telecommunications carriers and would not restrict profiling using the same types of consumer data by websites, network advertising services and other non-carriers.[121]

'Lawmakers Examine Privacy Practices at Cable, Web Firms,' *Wall Street Journal* (23 April 2009) (reporting that House of Representatives subcommittee hearings focused on efforts by Internet providers to collect and share data on consumers' behaviour to target online advertising and cable companies to target ads at subscribers via their set top boxes), available at: http://online.wsj.com/article/SB124050539070948681.html (last accessed 7 June 2010); Noyes, Andrew, 'House Internet privacy, data breach bills could merge,' *CongressDaily* (5 June 2009) (reporting that consumer privacy bills currently in Congressional subcommittees could be merged and that if adopted would give Web users greater protection in how information collected online is stored and used), available at: http://www.nextgov.com/nextgov/ng_20090506_2018.php (last accessed 7 June 2010) .

[111] For example, unlike the U.S. Constitution, California's state constitution provides more privacy protection than the federal constitution because it applies in business to consumer contexts that do not involve government actions. Cal. Const. art. I § 1; Hill v. NCAA, 865 P.2d 638 (California, 1994).

[112] Interview, NYMITY, Mary Ellen Callahan, 'Behavioral Advertising,' Hogan & Hartson LLP (January 2009) (Callahan Interview), available at: http://www.nymity.com/Free_Privacy_Resources/Privacy_Interviews/2009/Mary_Ellen_Callahan.aspx (last accessed 7 June 2010).

[113] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (COPPA).

[114] Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §§ 6801-6809.

[115] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified, as amended, in 42 U.S.C. § 1936 and other sections of the U.S. Code).

[116] Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 *et seq*.

[117] See Federal Communications Commission, About the FCC (About FTC), available at: http://www.fcc.gov/aboutus.html (last accessed 7 June 2010).

[118] 47 U.S.C. §222 (c) (requires telecommunications carriers to obtain customer approval to use, disclose or permit access to individually identifiable customer proprietary network information except to provide telecommunications services and related services or as required by law); 47 C.F.R. § 64.2003 (CPNI Regulation).

[119] King, FCLJ (2008), note 28, p. 276-281.

[120] King, FCLJ (2008), note 28, pp. 280-281.

[121] 47 U.S.C. § 222(a).

4.2.2. Consumer Protection and Privacy Regulation. Generally speaking, U.S. companies are free to operate their businesses and market to their customers and potential customers as they see fit as long as they do not engage in unfair or deceptive business practices or violate laws that regulate specific business practices.[122] The FTC is the leading federal consumer protection agency in this regard[123] and it enforces the federal statute that prohibits unfair or deceptive business practices that bars false or deceptive advertising.[124] The FTC could interpret this statute to cover consumer profiling that is unfair or deceptive, although it has not done so to date. Consumer privacy groups in the U.S. have filed a complaint with the FTC asking it to investigate privacy-intrusive practices of the behavioural advertising industry, claiming consumer profiling practices of the industry constitute unfair and deceptive business practices.[125] No law or FTC regulatory action currently requires behavioural advertisers to give consumers access to their personal information or profiles.[126]

Although Section 5 of the FTC Act has not been interpreted to require a website to have a privacy policy, a company's failure to follow its voluntarily adopted privacy policy may lead to an FTC enforcement action for deceptive practices.[127] Also, the FTC has found misuse of sensitive personal information by a company that has no privacy policy to be an unfair practice.[128] Because currently no U.S. law requires companies conducting consumer profiling for behavioural advertising purposes to adopt privacy policies related to profiling, companies may minimize consumer privacy challenges related to breaching their own privacy policies simply by refusing to adopt privacy policies. Alternatively, companies could adopt privacy policies designed to give them broad discretion to collect, use and share consumer data for consumer profiling and to deliver targeted advertising, giving them implied consent to transfer personal data and information about individual profiles to third-parties, such as network advertising partners, and reserving the right to change their policies without notifying consumers or obtaining their consent to the changes.[129]

Some have argued that data collection practices by behavioural advertisers used for consumer profiling involve conduct that is analogous to deploying spyware and may violate the federal Electronic Communications Privacy Act

---

[122] Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45 (Section 5). Deceptive practices include material misrepresentations or omissions that are likely to mislead reasonable consumers. Unfair practices are those that involve substantial harm to consumers where the harm is not reasonably avoidable by consumers and practices' benefits to consumers do not outweigh the harm. Callahan Interview (2009), note 112, p.1.

[123] See About FTC, note 117.

[124] See Federal Trade Commission Act (FTC Act), 15 U.S.C. §45(1) (Section 5).

[125] See generally, CDD Profiling Complaint, note 17.

[126] Regulation of specific marketing practices such as telemarketing and spamming further restrict marketing by behavioural advertisers to mobile customers. These marketing laws have been explored in other articles and are generally outside the focus of this article. See generally, King, FCLJ (2008), note 28 and Cleff, Dissertation, note 18.

[127] For example, the Federal Trade Commission used Section 5 of the FTC Act to prosecute a company for breaching its privacy policy by renting its customers' personal information to other companies for advertising purposes. Agreement Containing Consent Order, Gateway Learning Corp., File No. 042-3047 (FTC, 2003), available at: http://www.ftc.gov/os/caselist/0423047/040707agree0423047.pdf (last accessed 7 June 2010).

[128] Since 2001 the Federal Trade Commission has brought at least twenty-three enforcement actions against companies that failed to provide reasonable protections for sensitive consumer information and it has brought at least eleven enforcement actions since 2004 that relate to misuse of spyware. FTC, Prepared Statement of the FTC on Behavioral Advertising, Before the Senate Committee on Commerce, Science, and Transportation, Washington, D.C., p.8 (9 July 2008) (FTC Congressional Testimony), available at: http://ftc.gov/os/2008/07/P085400behavioralad.pdf (last accessed 7 June 2010).

[129] Solove et al. (2006), note 108, p. 32 (commenting that contracts often function "as a way of sidestepping state and federal law" that is designed to protect consumers' privacy). For example, contractual language to acknowledge consumers' consent to receive m-advertising or to use consumers' personal data to generate advertising could be inserted in standard form contracts that consumers have little choice but to sign in order to receive the desired service.

(ECPA) or the federal Computer Fraud and Abuse Act (CFAA).[130] Among other things, the ECPA prohibits unauthorized wiretapping and unauthorized accessed to stored electronic communications and the CFAA prohibits computer hacking. To the extent that courts have considered claims of privacy violations by online advertising companies including claims under these statutes, they have found no privacy violations.[131] However, a recently filed privacy lawsuit will give a federal court the chance to address this issue in the behavioural advertising context. This lawsuit was filed by customers of an ISP who claim the ISP installed spyware devices from NebuAd, a behavioural advertiser, without providing adequate notice and that this conduct violated their privacy under the tort of intrusion into the seclusion of their private affairs. They also claim the ISP violated federal wiretap and computer hacking laws.[132]

4.2.3. U.S. Data Privacy Gaps. There is a vast difference between EU and U.S. regulatory frameworks when it comes to consumer privacy and data protection. Generally speaking, five regulatory gaps have been identified in the U.S. system regarding the collection and dissemination of PII in that the vast majority of companies engaged in e-commerce are not legally required to: "(1) create a comprehensible and succinct privacy policy detailing their PII practices; (2) post a conspicuous link to any privacy statement; (3) disclose the external uses of PII (either collected actively or passively); (4) disclose visitor consent options regarding PII collection and dissemination and privacy policy amendments; or (5) refrain from widely disseminating PII to the highest bidder on the open market."[133]

With few exceptions, all five of these gaps exist with respect to regulation of consumer profiling by the behavioural advertising industry in the U.S. However, there are some exceptions where federal regulation closes the gaps. These exceptions apply to websites that collect the PII of children under 13, to the collection and use of protected health information by health care providers and to the collection and use of consumers' information by financial service companies. Federal regulation of these industry sectors gives consumers specific privacy rights and may require the covered entities to post a privacy policy.[134] Only the state of California has passed generally applicable legislation that requires most companies that do business in California to post an online privacy policy conforming to state privacy statutes.[135] So, generally speaking, with the exception of California, a business engaged in consumer profiling for behavioural advertising purposes is not required by law to post a privacy policy, and if it does, the terms of that policy are largely left to its discretion so long as its actions are not found to be unfair or deceptive practices. Further, studies of privacy policies posted by e-businesses show that few companies have chosen to

---

[130] Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2510 *et seq.;* Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 *et seq*.; Ng, note 43, pp. 374-382 (arguing the ECPA, which prohibits interception or unauthorized access to electronic communications but does not directly address online behavioural advertising (OBA), and the CFAA or analogous state laws that specifically regulate spyware could be used to regulate OBA). See also, Baldas, T., 'Advertiser tracking of Web surfing brings suits,' *The National Law Journal* (2 Mar. 2009), available at: http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202428674349&slreturn=1 (last accessed 7 June 2010).

[131] Hotaling, note 13, pp. 549-550 (footnote146).

[132] Davis, W., 'Customers Sue ISP for Installing NebuAd 'Spyware,' Offering Defective Opt-Outs, *MediaPostNews* (28 Jan. 2010), available at: http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=121522 (last accessed, 7 June 2010).

[133] Ciocchetti (2008), note 109, p. 610.

[134] Ibid. pp. 612-615 (commenting that Congress has chosen not to mandate the posting of privacy policies for most companies operating Websites and that the threat of FTC scrutiny on broken privacy promises gives companies incentives to fail to post a privacy policy or to create a privacy policy that includes legalese and loopholes designed to avoid breaking any promises).

[135] California Business and Professional Code § 22575 (requiring anyone collecting PII from a resident of the state to post a privacy policy, identify types of PII collected, disclose categories of external parties that information may be disclosed to, describe any policy allowing review or requested changes to PII, provide notice of how the company may alter its policy and include the effective date of the policy). See also Cal. Civ. Code § 1798.83 (requiring, upon request, companies that disclose PII to third parties for direct marketing purposes to disclose the categories of PII the company has disclosed to third parties and the names of all third parties that received PII from the company for direct marketing purposes).

restrain their freedom to use consumers' personal data for reasons unrelated to its collection, to make material amendments to their privacy policies, or to sell consumers' personal data to other businesses.[136]

As compared to the broader scope of profiling and behavioural advertising, the mobile context brings with it a higher level of federal regulation to protect consumers' privacy and data protection and smaller regulatory gaps. For example, a mobile carrier's involvement in consumer profiling and behavioural advertising brings with it regulatory limits on the use and disclosure of subscribers' CPNI, a highly sensitive form of PII. CPNI includes mobile subscriber-identifiable information about phone numbers dialed and the geographic location of the person who made or received the call (location data). [137] A carrier needs opt in consent from a subscriber to share his or her CPNI with third-party mobile advertisers who may desire to use that data to construct customer profiles for behavioural advertising purposes.[138] The CPNI regulations restrict uses of CPNI that otherwise could be used to develop highly sensitive customer profiles based on mobile phone users' geographic locations at particular points in time such as targeting consumers for location-based services and m-advertising. The use of phone numbers dialed or numbers from which calls are received is also restricted as CPNI. Otherwise this data could also be used to develop highly sensitive customer profiles as it may reveal the names of health care providers, religious counselors, sexual partners, etc.

Thus the regulatory gap is narrower in the case of CPNI uses for behavioural advertising because it is already subject to federal regulation designed to ensure subscribers give their informed consent before carriers disclose CPNI to third parties, such as joint venture partners or independent contractors, for marketing purposes. However, once a consumer gives consent for carrier disclosure of CPNI, the consumer has no right under the CPNI regulations to be notified of, or to refuse consent, to further transfers or uses of the consumer's CPNI, whether for behavioural advertising or other purposes.[139] Further, most behavioural advertisers are not regulated telecommunications carriers covered by the CPNI rules and are not covered by industry-specific laws requiring them to adopt or post a privacy policy. If behavioural advertisers use consumer profiling and they voluntarily adopt privacy policies, they are free to craft the terms of that policy and reserve broad discretion to use consumers' data for profiling, to freely amend their policies, and to share or sell consumers' data and/or profiles to third parties without notice to affected consumers or obtaining their consent. Of course the general regulatory framework for mobile spam and telemarketing solicitations will apply and set some parameters to protect mobile users' privacy to be free from fraudulent or abusive forms of advertising solicitations, however, these regulations do not protect mobile users' from unwanted customer profiling or require fair information practices by those engaged in behavioural advertising.

In sum, U.S. privacy and data protection laws fall far short of providing a comprehensive federal privacy and data protection framework for behavioural advertising similar to that found in the European Union. No generally applicable data protection or privacy regulation exists in the U.S. to give consumers privacy and data privacy rights

---

[136] Ciocchetti (2008), note 109, p. 597 (reporting the study of 25 most visited e-commerce websites in the U.S. which showed the vast majority reserve the right to collect PII and disseminate the information to unrelated third parties). He believes federal legislation is needed to require companies to either post a clear and conspicuous privacy policy that describes seven key PII practices in plain English or to associate (tag) their name to each piece of data they disseminate, with purchasers of the tagged PII being legally required to identify the seller whenever they solicit individuals identified by the purchased PII. It is argued such legislation will result in social pressure that will lead companies to draft and post better privacy policies. Ibid. p. 627.

[137] 47 U.S.C. § 222 (h)(1) (defining the scope of CPNI to include information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service … and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship). CPNI does not include collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed. 47 U.S.C. § 222 (h)(2).

[138] See Telecommunication Carriers' Use of Customer Proprietary Network Information and Other Customer Information, *Report and Order and further Notice of Proposed Rule-Making*, 22 F.C.C.R. 6927, pp. 22-23 (2007) (2007 CPNI Order) (discussing the modification of the FCC rules to require carriers to obtain opt in consent n the form of express prior authorization from a customer before disclosing that customer's CPNI to a carrier's joint venture partner or independent contractor).

[139] King, FCLJ (2008), note 28, at pp. 276-280.

similar to those EU citizens have under the Data Protection Directive and no laws currently restrict the use of computer profiling by behavioural advertisers in order to protect consumers' privacy. The privacy gaps listed in Section 4.1.3 of this article that have not yet been specifically addressed in EU legislation also have not yet been addressed in U.S. legislation or in enforcement actions for unfair or deceptive practices brought by the FTC.

This article now turns to regulatory developments that reflect the increasing focus of EU and U.S. regulators on protecting consumers from privacy-intrusive practices associated with behavioural advertising and profiling. To date both EU and U.S. regulators have been hesitant to legislate privacy protections for profiling by behavioural advertisers that could unnecessarily burden this new industry. Instead, regulators have endeavored to support industry self-regulation and technological innovations that aim to protect consumers' privacy. Industry self-regulation is attractive to the behavioural advertising industry because it can be global in nature and does not depend on any one regional or national regulatory framework.

5. Recent EU and US Regulatory Developments Addressing Consumer Profiling and Behavioural Advertising

There is ongoing action by the European Commission to further implement the two key EU regulatory instruments on data protection: the Data Protection Directive and the E-Privacy Directive.[140] Viviane Reding, former Information Society and Media Commissioner, has recently been appointed the EU's new Commissioner for Justice and Fundamental Rights.[141] Commissioner Reding has taken on the task of revising the EU's data protection rules.[142] Also, the European Commission formed a new group to address companies' collection and use of customers' personal data and problems related to behavioural advertising.[143] Additionally, the EU recently adopted a package of legislation reforming regulation of the telecommunications industry. This legislation amends the E-Privacy Directive in ways that will impact behavioural advertising practices. Also, the Council of Europe's Directorate General of Human Rights and Legal Affairs published a draft recommendation on data protection in the framework of profiling.[144] In the U.S., the Federal Trade Commission (FTC) issued industry-specific guidance for online behavioural advertisers to help them self-regulate, although neither Congress nor the FTC have adopted any binding legislation or regulation.[145] These recent developments are discussed next.

5.1 The EU's Telecoms Reform Package. In 2009, the EU Telecoms Reform Package was adopted. It will require telecom operators and other businesses, including behavioural advertisers, to better inform consumers about their use of cookies or other online tracking technologies.[146] The EU Telecoms Reform Package amends the E-Privacy Directive to require advertisers and others to give consumers clear and comprehensive information in accordance with the Data Protection Directive about the purposes of any personal data processing before storing information or

---

[140] See generally, Data Protection Directive, note 35; E-Privacy Directive, note 56.
[141] 'EU justice chief plans civil code, privacy laws,' EurActiv.com (21 Dec. 2009).
[142] Ibid.
[143] 'Commission forms industry body to solve behavioural advertising problems,' *OUT-LAW News* (16 Nov. 2009) (reporting the formation of the Stakeholder Forum on Fair Data Collection, a collection of businesses who have to outline their plans for protecting consumers' information), available at: http://www.out-law.com/page-10526 (last accessed 7 June 2010).
[144] See generally, CE Draft Recommendation on Profiling, note 5.
[145] As mentioned earlier in this paper, a formal complaint was filed with the FTC in April 2010 by consumer privacy organizations asking the FTC to investigate businesses engaged in consumer profiling practices that are alleged to be unfair or deceptive practices in violation of Section 5 of the FTC Act. The scope of the requested investigation includes behavioural advertisers, third-party data providers, and other businesses providing ad-exchange systems that support the behavioural advertising industry and facilitate real-time consumer profiling. See generally, CDD Profiling Complaint, note 17. The Complaint provides a comprehensive description of the behavioural advertising industry and the development of real-time profiling technologies. The Complaint is still pending as of the publication date of this paper.
[146] News Release, European Commission welcomes European Parliament approval of sweeping reforms to strengthen competition and consumer rights on Europe's telecoms markets, Brussels, IP/09/1812 (24 Nov. 2009).

gaining access to information already stored on their terminal equipment, such as computers and mobile phones.[147] One effect of the amendment is to require advertisers and other businesses to obtain consumers' consent to access or store information on their terminal equipment even if doing so does not require using a regulated electronics communications network such as a telephone carrier.[148]

To the extent that access to or storage on a user's terminal equipment occurs using an electronic communications network, notice and consent obligations already existed before the recent amendments to the E-Privacy Directive, although only opt out notice was required.[149] The amendments, on first reading, appear to change this to require opt in consent, although this is not clear. The preamble to the amendments creates doubt on this point by commenting that a consumer must be provided with a "right to refuse" that "should be as user-friendly as possible" before cookies may be placed on the user's computer or mobile device in order to facilitate storage and access to information, like the storage and access of cookies that typically supports behavioural advertising.[150] Further, some forms of cookies used by behavioural advertisers, such as cookies that do not store PII, may not be covered by the new rules.[151] Some commentators believe this requirement to obtain users' consent before placing cookies on their machines could unduly restrict the behavioural advertising industry.[152] The amendments to the E-Privacy Directive become effective through implementation in Member States' laws by May 2011. The process of adopting the amendments through national law may resolve some of the current ambiguities about the type of notice that will be required to store or access cookies under the E-Privacy amendments.[153]

5.2 Council of Europe's Draft Recommendation on Profiling. In 2010 the Council of Europe's Directorate General of Human Rights and Legal Affairs issued a draft recommendation that outlines broad principles and minimum consumer rights designed to protect individuals in the context of automatic processing of their personal data by individuals and bodies that use profiling in the field of information services (Draft Recommendation).[154] The Draft Recommendation is designed to guide those who participate in and use profiling and covers software designers and suppliers of software for electronic communications terminal equipment (e.g., mobile phones and computers); designers of profiles (e.g., behavioural advertisers); Internet Access providers (ISPs), and other information society service providers (e.g., telecommunications carriers).[155] Essentially the Draft Recommendation provides general principles and minimum protections for data protection and privacy in the context of profiling. It does not, however,

---

[147] See EU Telecoms Reform Package, note 59 (incorporating E-Privacy Act Amendments, Art. 5(3)). These amendments expand the requirement to give notice and obtain the user's consent to access or store information on the user's terminal equipment to all situations where this occurs, even if the access or storage does not involve using an electronic communications network. Exceptions permit any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user of the service. Ibid.

[148] Ibid.

[149] Ibid. (based on comparison of Art. 5(3) of the E-Privacy Directive as adopted in 2002 with the amended version of Art. 5(3) as adopted in the EU Telecoms Reform Act).

[150] EU Telecoms Reform Package, note 59, at para. 66. The preamble of the EU Telecoms Reform Package anticipates that the user's consent to processing of personal data may be expressed by appropriate browser settings or other applications where this is technically possible. Ibid.

[151] Nauwelaerts, W., 'EU e-Privacy Directive and Cookies: The Consent Requirement May Not Be as Broad as Believed,' Hogan & Hartson (16 Nov. 2009), 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 7 June 2010).

[152] Marshall, J., 'EU Proposal Could Cripple Common Web Ad Practices,' *ClickZ News UK & Europe* (6 Nov. 2009).

[153] 'Europe Approves New Cookie Law,' *The Wall Street Journal* Blogs (11 Nov. 2009), available at: http://blogs.wsj.com/digits/2009/11/11/europe-approves-new-cookie-law/ (last accessed 7 June 2010); Member states shall adopt and publish by 25 May 2011 the laws, regulations and administrative provisions necessary to comply with the directive 2009/136, see EU Telecoms Reform Package, note 59, article 4(1)

[154] See generally, CE Draft Recommendation on Profiling, note 5.

[155] Ibid. p. 4 (para. 2).

provide industry specific guidance such as the U.S. industry-specific guidance for online behavioural advertising that is discussed in Section 5.3.[156]

The general principles and minimum consumer rights that behavioural advertisers need to know are outlined in an Appendix to the Draft Recommendation. This Appendix defines important terms, addresses the scope of the recommendation, outlines conditions for personal data collection and processing using profiling and outlines the types of disclosures of information that should be provided to the data subject.[157] It also discusses the privacy and data protection rights of data subjects, remedies for data protection violations.

5.2.1 Definitions and Scope. The definition of profiling in the Draft Recommendation is broad enough to include all forms of customer profiling for the purposes of delivering targeted advertising to customers: "Profiling means an automatic data processing technique that consist[s] of applying a 'profile' to an individual, namely in order to take decisions concerning him or her; or for analysing or predicting personal preferences, behaviours and attitudes."[158] The scope of the Draft Recommendation includes all processing of personal data using profiling by the private and public sectors, so it will apply to behavioural advertising and profiling of mobile users.[159] The Draft Recommendation advocates respect for the fundamental rights and freedoms of individuals including guaranteed rights of personal data protection and it prohibits arbitrary measures or decisions contrary to the law.[160] It advises Member States to encourage the development of privacy-enhancing technologies "in particular software which does not permit the profiling of users without their free, specific and informed consent."[161]

5.2.2 Application of the Data Protection Directive. The Draft Recommendation incorporates the general requirements of the EU's Data Protection Directive for the lawful processing of personal data (e.g., fairness, legitimate purpose, proportionality, data adequacy and data security, etc.).[162] It requires providers of information society services to ensure, by default, non-profiled access to their services.[163] It would therefore prohibit a mobile carrier or an ISP from requiring consumers to give their consent to be profiled for behavioural advertising purposes as a condition of using the carrier's or ISP's services. Further, the Draft Recommendation states that the distribution of monitoring software for profiling purposes without the knowledge of the person to be observed or monitored should be permitted only if this is expressly allowed under domestic law comprising appropriate safeguards.[164] It defines sensitive data consistent with the Data Protection Directive and prohibits processing sensitive data for profiling purposes except if these data are necessary for the lawful and specific purposes of processing with appropriate safeguards under domestic law.[165] Personal data that reveals "racial origin, political opinions or religious or other beliefs, as well as personal data on health, sex life or criminal convictions" and "other data defined as sensitive by domestic legislation" (essentially data that has been defined as special categories of data and considered sensitive data under the Data Protection Directive) may not be processed to create consumer profiles except when permitted by law and with the consumer's explicit consent. Even so, processing of sensitive data for profiling must be necessary for purposes of processing and consistent with appropriate safeguards under domestic law..[166]

---

[156] The Draft Recommendation recommends that Member States take steps to adopt its principles through law and practice. Ibid. p.4 (para. 1). It also encourages promotion of self-regulation mechanisms such as codes of conduct that ensure respect for privacy and data protection and to put in place the technologies that further its principles. Ibid. p. 4 (para. 3).
[157] Ibid. pp. 1-10.
[158] Ibid. p. 5 (para. 1(e)).
[159] Ibid. p. 5 (para. 2).
[160] Ibid. p. 6 (para. 3).
[161] Ibid. p. 6 (para. 3.3).
[162] Ibid. p. 6 (para. 4); p. 7, B; p. 10 (para. 8).
[163] Ibid. p. 7 (para. 4.7).
[164] Ibid. p. 7 (para. 4.8).
[165] Ibid. p. 5 (para. 1(b), p. 7 (para. 4.11).
[166] Ibid. pp. 6, 7 (para. 4.4, C. para. 4.11).

5.2.3 Consumer Notice of Profiling. The Draft Recommendation requires that consumers (data subjects) whose personal data is collected by a business (the controller, such as an advertising network or a website that tracks and publishes ads, etc.) give consumers the following minimum information with respect to consumer profiling:

a. the existence of profiling;
b. the purposes for which the profiling is made;
c. the effects of applying the profiling to the data subject;
d. the categories of personal data used;
e. the identity of the controller and if necessary his/her representative;
f. the existence of appropriate safeguards.[167]

Further, the Draft Recommendation requires giving "all information that is necessary for guaranteeing the fairness of recourse to profiling" to the person whose personal data is collected for profiling. Information that must be disclosed includes: those with whom personal data will be shared; the purposes of the sharing; the possibility that the person may withdraw his or her consent; conditions for persons to access, object, and/or correct their personal data; whether replying to questions used to collect personal data are compulsory or optional and the consequences of not replying to the questions; and the duration of storage.[168] These provisions require behavioural advertisers to tell consumers if they will share their personal data with a network advertising service for the purposes of delivering targeted advertising across multiple websites and whether the consumer may have access to websites that use behavioural advertising without consenting to targeted advertising, third-party personal data sharing, etc.

5.2.4. Consumers' Right to Refuse Profiling. The Draft Recommendation only allows processing of personal data for profiling purposes if it is permitted by law and the data subject (consumer) has given his or her free, specific and informed consent.[169] Generally this means behavioural advertisers need consumer consent to collect consumers' personal data and to use it to generate consumer profiles. In the case of sensitive data, that consent must be explicit. There are exceptions allowing processing of personal data without consent including situations where it is provided by law or necessary to performance of a contract to which the data subject is a party, etc. Even if anonymous data is used for consumer profiling, to the extent that profiling generates new personal data, behavioural advertisers need consumer consent to apply a consumer profile to an individual consumer.[170]

5.2.5. Other Consumer Rights. Under the Draft Recommendation, consumers (data subjects) have the right to access personal data concerning them, including "knowledge of the profile and of correction, deletion or blocking" which shall not be limited unless prescribed by law and necessary to protect state security or public safety.[171] In the behavioural advertising context, although there is a requirement to give consumers information about the existence, purposes and effects of profiling, unless the profiles are personal data, consumers do not have the right to access information about individual profiles applied to them or descriptions of the market segments to which they have individually been assigned.[172] Consumers would have a right to object to profiling that leads to a decision that has legal or other significant effects for the consumer. Presumably, if profiling for behavioural advertising purposes results in unfairness or discrimination, the consumer will be able to object.[173] For example, if behavioural advertising applies a profile to a consumer that is the sole reason the consumer is denied the right to participate in favorable offers for insurance or credit, the consumer could challenge the accuracy of the profile as unfairly excluding him or her based on erroneous information or argue that the profile discriminates on the basis of race, etc.

---

[167] Ibid. p. 8 (para. 5.1).
[168] Ibid. p. 8 (para.5.1(h)).
[169] Ibid. p. 6 (para. 4.4). Whether opt in or opt out consent is required is not addressed by the Council of Europe's Draft Recommendations, but presumably interpretations of these terms would be consistent with the requirements of the Data Protection Directive.
[170] Ibid. p. 2 (para. 7) (commenting that "profiles, when they are attributed to a data subject, make it possible to generate new personal data").
[171] Ibid. p. 9 (para. 6.4).
[172] See earlier discussion that adequate protection of personal data and privacy requires consumers to have access to the profiles applied to individual consumers, text accompanying notes 39-43.
[173] CE Draft Recommendation on Profiling, note 5, p. 9 (para. 6.7).

The Draft Recommendation is not legally binding. Instead it recommends that Member States adopt its principles in domestic law.[174] It also encourages Member States to provide appropriate sanctions and remedies for breach of the principles set out in the Draft Recommendation.[175] It advises Member States to require independent authorities to ensure compliance with their domestic legislation implementing its principles.[176]

5.2.6 Strengths and Weaknesses of the Draft Recommendation. The Draft Recommendation makes an important contribution to the discussion about protecting privacy and personal data in today's world where ubiquitous computing and automatic profiling challenges existing regulatory frameworks and threatens to strip consumers of any real control over their privacy and personal data. As an international statement about the privacy and data protection principles that should apply in the context of profiling, it provides leadership in the global effort to protect consumers from abusive uses of profiling. The Draft Recommendation provides privacy protecting principles that will guide regulators to address most the privacy gaps that currently exist with regard to consumer profiling and behavioural advertising. However, it does not attempt to apply those principles to specific business practices such as profiling for behavioural advertising or related to mobile customers.

One weakness in the Draft Recommendation is that Member Countries must agree to implement these principles through their domestic laws. This may lead to inconsistent regulation by Members of the Council of Europe. Some countries may choose to implement it, while others will choose not to do so or will implement it inconsistently with other adopters. A second weakness is that the Draft Recommendation was created before the anticipated review and revision of the Data Protection Directive. A separate source of privacy and data protection law may not be necessary, assuming the Data Protection Directive is revised to address computer profiling by behavioural advertisers and the revised directive is implemented by the Member States. A third weakness is that the Draft Recommendation applies the general notice and consent approach to data protection to the profiling context despite contemporary criticism that the notice and consent approach does not adequately protect consumer privacy and data protection in today's ubiquitous computing environment.[177] Hopefully, the process to review the Data Protection Directive will explore the continuing validity of the notice and consent approach to data protection.[178] To the extent that the Draft Recommendation supports opt in mechanisms for obtaining consumer consent for profiling, it avoids some of the privacy concerns related to self-regulatory approaches for behavioural advertising that often depend on privacy policies and notice and consent mechanisms that use opt out mechanisms.[179] On the whole, the Draft Recommendation is a well thought-out proposal and important statement about consumer privacy that will help

---

[174] Member States of the European Union transfer national legislative and executive powers to the Council of the European Union, the European Parliament and the European Commission in specific areas under European Union law. In contrast, Member States that are members of the Council of Europe commit themselves through conventions developed by the Member States working together at the Council of Europe that are instruments of public international law. Non-EU countries may sign such conventions so the membership of the Council of Europe is broader than EU membership.

[175] Ibid. p. 9 (para. 7).

[176] Ibid. p. 10 (para. 9) (providing that Member States may require advance notification or prior checking to the supervisory authority for processing that uses profiling and entails special privacy and data protection risks).

[177] "[I]n the brave new digital world where data collection opportunities are many and data use opportunities are rich, "notice" is failing when it comes to privacy." 'On notice, consent, and radical transparency,' *The Privacy Advisor*, p. 20 (Sept. 2009) (no author provided). See also, Lukovitz, K., 'FTC's Focus Re Privacy Issues Emerging,' MediaPost News (29 Jan. 2010) (reporting that the FTC is exploring whether a more complete solution to protect consumers privacy is needed that goes beyond an approach based on the "notice and choice" concept of information privacy).

[178] "Operating without consumers' 'knowledge or [or] authorization,' [behavioural targeting or BT] technology undermines the ability of users to consent by failing to provide effective notice of its existence." Hotaling, note 13, pp. 551-560.

[179] Ibid. The question of whether notice and choice mechanisms are adequate to protect consumers' privacy in ubiquitous computing environments and this era of autonomic computing is an important question and one that deserves much discussion and analysis. See generally, sources referenced in note 177; Sterritt et. al, 'A concise introduction to autonomic computing,' 19 *Advanced Engineering Informatics*, pp. 181-187 (2005). As such, it is beyond the scope of this paper.

shape the discussion about whether, and how, to regulate automatic profiling to protect consumers' privacy and personal data. It is the most insightful and comprehensive statement to date by an international body on the privacy implications of profiling.

5.3 Federal Trade Commission's Industry-Specific Guidelines

In 2009 the staff of the U.S. Federal Trade Commission (FTC) issued a report urging businesses participating in online behavioural advertising (OBA) to follow four principles in order to protect consumers' privacy when engaging in online behavioural advertising.[180] The FTC's Staff Report (FTC Guidelines), which is not legally binding and instead provides guidance for companies to self-regulate, sets four general principles for online behavioural advertising: 1) transparency and consumer control; 2) reasonable security and limited data retention for consumer data; 3) affirmative express consent for material changes in existing privacy promises; and 4) affirmative express consent, or alternatively prohibition against, using sensitive data.[181]

5.3.1 Scope of the FTC Guidelines. The FTC defines OBA, and thus the scope of its guidance, to include: "the tracking of a consumer's online activities over time – including the searches the consumer has conducted, the Web pages visited, and the content viewed – in order to deliver advertising targeted to the individual's interests."[182] Significantly advancing the relevant privacy discussion, the scope of the FTC Guidelines protects "consumer data" including both PII and non-PII.[183] In so doing, the FTC Guidelines avoids one of the significant limitations of attempting to apply the EU's existing regulatory system to consumer profiling by behavioural advertisers, which is that the EU's data protection legislation was primarily designed to regulate the processing of PII and is not generally applicable to address the important privacy concerns that arise of uses of non-PII for consumer profiling.[184]

On the other hand, the FTC Guidelines narrowly define OBA and exclude from the application of its four principles two forms of targeted advertising: 1) "first party" or "intra-site" advertising, where no data is shared with third parties, and 2) "contextual advertising," where an ad is based on a single visit to a web page or a single search query.[185] For example, the FTC Guidelines cover a situation involving a travel website that offers airline tickets and a website that sells clothing when both have an arrangement with a network advertiser[186] to provide targeted advertising to their visitors because the tracking and delivery of advertising to the consumer takes place over multiple websites and over time. When the customer first conducts research on the travel website searching for airline reservations from Amsterdam to New York City and then later visits the clothing website where she is served a targeted ad offering her hotel reservations and theatre tickets in New York City, the ad delivery on the travel website is OBA covered by the Guidelines.[187]

However, the FTC Guidelines do not apply to "first party" targeted advertising delivered to the consumer on a travel website, even if the consumer makes multiple visits to the travel website, as long as the travel website does not share any consumer data with third parties. For example, an offer on a travel website to rent a model of a car that is based on previous search queries on the travel site by the consumer is not OBA, as long as the travel site does not share any consumer data with third parties (such as network advertising companies). This is so even though the consumer's behaviour on the travel site has been tracked by the travel site and tailored to reflect the dates that the

[180] See generally, FTC Guidelines, note 60.
[181] FTC Guidelines, note 60, pp. 46-47.
[182] Ibid. p. 46.
[183] Ibid. pp. 21-26 (adopting the view that the principles in the FTC Guidelines apply to any data collected for online behavioural advertising that could reasonably be associated with a particular consumer or with a particular computer or device, even if the data if non-PII).
[184] See generally, Dinant et al., note 6, pp. 30-31.
[185] FTC Guidelines, note 60, pp. 26-30.
[186] "Ads from network advertisers are usually delivered based upon data collected about a given consumer as he or she travels across the different Web sites in the advertising network. An individual network may contain hundreds or thousands of different, unrelated Web sites and an individual Web site may belong to multiple networks." FTC Guidelines, note 60, p. 3 (note 5).
[187] Ibid. p. 3.

consumer has searched for airline reservations on the site and inferences made by the site about the consumer's likely travel destination. The FTC explains that the second example involves tracking only by the travel site and not across multiple websites, which according to the FTC Guidelines, is first party advertising and not OBA that is less of a privacy concern.

Additionally, the FTC Guidelines do not apply to a targeted ad sent to a consumer that is based on a single search query or a single visit to a web page, because this is "contextual advertising," as opposed to OBA. For example, if a consumer is shown an advertisement for travel clothing solely because she has visited a website that sells travel clothing or has used a search engine to find stores that sell travel clothing, this is not OBA within the FTC's definition because it does not rely on the collection of detailed information about the consumer's actions "over time."[188] The FTC Guidelines exclude first-party and contextual advertising from its guidance on OBA having concluded that first-party and contextual advertising do not raise the same level of privacy and data protection concerns for consumers, are more likely to be consistent with consumers' expectations, and are less likely to lead to consumer harm compared to practices involving the sharing of consumer data with third parties or across multiple websites.

5.3.2. Notice and Consent. The Guidelines require companies engaged in OBA to give consumers notice that their data is being collected on the site for use in providing tailored advertising and a choice whether or not to have their data collected for this purpose. The Guidelines generally allow companies to choose whether to provide opt in or opt out notice and consent mechanisms. There are two cases where the FTC says consumers should have the right to be asked for opt in consent: 1) companies should obtain affirmative express consent from consumers before collecting sensitive data, and 2) companies should obtain affirmative express consent before changing a privacy policy in order to use previously collected data in a manner materially different from promises made when the data was collected. Recognizing that privacy policies have become long and difficult to understand and may not be an effective way to communicate information to consumers, the FTC encourages companies to design innovative ways that are outside of the privacy policy to provide behavioural advertising disclosures and options for choice to consumers. For example, it may be effective to generate a message such as "why did I get this ad?" for a consumer that is located near an advertisement and links to the relevant section of a privacy policy explaining how data is collected for targeting advertising.[189]

5.3.3. Strengths and Weaknesses of the FTC Guidelines.

The primary strength of the FTC Guidelines is that it clearly explains the current practices of behavioural advertising and identifies many important consumer privacy implications in the process of articulating its self-regulatory principles. The Guidelines include comprehensive reference to information about behavioural advertising from the viewpoint of multiple stakeholders and clear examples of how consumers' information is collected and used by behavioural advertisers to generate targeted advertising. This useful and detailed background information will be helpful to both industry self-regulators and government regulators as they work to address the specific privacy concerns related to consumer profiling and the behavioural advertising industry.

The most critical weakness of the FTC Guidelines is that it recommends fair information practices for online behavioural advertising without addressing the consumer privacy or data protection concerns related to the creation and use of consumer profiles for behavioural advertising purposes. The Guidelines do not addresses two of the most important questions: 1) whether automatic profiling generally raises consumer privacy issues, and 2) whether creation of consumer profiles that are applied to individual consumers creates personal data, and if so, what rights consumers should have to learn about the consumer profiles that have been applied to them. On the other hand, as discussed below, application of the Guidelines is not limited to personally-identifiable information (PII), so it may be applicable in situations where anonymous data is used in the targeting process.

There are several other deficiencies in the FTC Guidelines. First, the Guidelines do not recommend that companies obtain consumers' specific consent before they share consumers' data with third-parties. This allows companies to

[188] Ibid. pp. 26-30
[189] Ibid. p. 35.

use general opt out notices to establish consumers' consent including an inference that consumers have consented to the sharing of their data with third parties, unless they have taken affirmative action to the contrary (except in the cases of sharing sensitive data or sharing that is a material departure from the company's policy when the data was collected).[190] Given that studies have shown that opt out notice and consent mechanisms are unlikely to result in truly informed consent and that few consumers even read these notices, this self-regulatory choice does not adequately protect consumers' privacy.[191] Failure to effectively limit third-party data sharing will enable creation of comprehensive databases containing consumer tracking data that spans long time periods, combines data collected by multiple websites and combines data from other on and offline sources. Such databases can be data mined enabling the creation of detailed individualized profiles.

Second, the FTC Guidelines do not include any enforcement mechanisms and instead indicate that companies should adopt meaningful enforcement mechanisms. Of course, as discussed previously, the FTC may use its statutory authority to regulate unfair or deceptive practices and seek injunctions or fines against companies that violate their own privacy policies or fail to secure sensitive customer data or otherwise engage in abusive practices. Further, some collections and uses of consumer data are already regulated by industry-specific data protection laws. For example, as discussed earlier, in the context of profiling by behavioural advertisers directed at mobile users, carriers must obtain opt in consent from users to share users' geographic location data (a form of CPNI) with non-affiliate companies for the purpose of constructing profiles for behavioural advertising.

Third, the Guidelines do not define sensitive data, although they provide a few examples of sensitive data such as financial data, data about children, health information and precise geographic location data. The inclusion of geographic location data as sensitive data is important to protect the privacy of mobile users. Nor do the Guidelines address whether there is a need to restrict the creation of sensitive marketing segments to be used for customer profiling purposes, although they to recognize that combination of information that are anonymous by themselves may constitute a highly detailed and sensitive profile that is potentially traceable to the consumer. [192]

Fourth, the Guidelines do not expressly address behavioural advertising directed at mobile customers. This is significant because behavioural advertisers may track users' mobile behaviour and locations for profiling purposes, yet the scope of the Guidelines is limited to behavioural advertising that tracks consumers' traditional online activities. Although a complaint was recently filed with the FTC by consumer privacy advocates requesting that the Guidelines be revised to include behavioural advertising involving mobile users, the FTC has not yet revised its Guidelines to address profiling practices that may be unfair or deceptive.[193] For targeted advertising that is not within the scope of OBA addressed in the FTC Guidelines, the FTC advises companies to develop alternative methods of disclosure and consumer choice that will satisfy the four principles in the Guidelines.

In sum, both the Draft Recommendation and the FTC Guidelines significantly address the privacy gaps in the EU and U.S. regulatory frameworks that leave consumers vulnerable to privacy-intrusive profiling by behavioural advertisers. However, neither the Draft Recommendation nor the FTC Guidelines give consumers any direct legal rights in this context, as the Draft Recommendation is not yet law and the FTC Guidelines have no binding effect.

---

[190] Ibid. p. 47.

[191] See Telecommunication Carriers' use of Customer Proprietary Network Information and Other Customer Information, Report and Order and Further Notice of Proposed Rulemaking, 22 F.C.C. Record. pp. 6927, 6948 (2007) (Federal Communications Commission characterizes "opt out" notices and consent as vague and ineffective).

[192] The FTC provides a hypothetical example of such a sensitive profile that is based on a 2006 incident involving AOL. In this incident, for research purposes, AOL made public approximately 20 million search queries from which subscriber names and user IDs had been replaced with identification numbers in order to protect the searchers' identities. Using this anonymized data, the media was able to identify at least one individual subscriber and other Internet users claimed to be able to identify others. FTC Guidelines, note 60, pp. 22-23 (footnote 51).

[193] See CDD Complaint of Unfair or Deceptive Mobile Marketing Practices, note 94; News Release, "Consumer Groups Petition Federal Trade Commission to Protect Consumers from Mobile Marketing Practices Harmful to Privacy", Center for Digital Democracy (13 Jan. 2009), available at: http://www.democraticmedia.org/node/397 (last accessed 7 June 2010).

This situation is a significant concern for mobile customers and the privacy gaps in both the EU and U.S. regulatory frameworks need to be addressed.

6. Conclusions

Many consumers will choose to receive behavioural advertisements generated by advertisers who use consumer profiling to produce highly targeted advertising. Consumers may say "yes" to behavioural advertising because it promises more relevant advertisements tailored to their individual interests, may save them time by delivering ads at the right time and place, and may alert them to money-saving opportunities that they otherwise may not discover. Generally speaking, informed consumers should have the freedom to choose to have their online and mobile behaviour tracked by advertisers and to have this information and other data about them processed by advertisers using consumer profiling technologies to generate targeted ads promoting products and services. As long as behavioural advertising practices comport with consumer protection standards and are not unfair or deceptive, advertisers should have the freedom to use profiling technologies to enhance their market segmentation and generate targeted advertising to consumers who want to receive such ads.

Consumer protection is a goal of both EU and U.S. laws. For example, both regulatory environments generally protect consumers from unfair or deceptive practices. Further, EU legislation separately guarantees privacy and personal data protection for its citizens. U.S. law also includes some minimal privacy and data protection rights for consumers under its prohibitions on unfair or deceptive practices or industry-specific legislation. However, as analysed earlier in this article, privacy and data protection 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. This article asserts that a regulatory environment for business that does not offer adequate protections for privacy and personal data fails to provide minimum consumer protections.

The Council of Europe's Draft Recommendation on Profiling (Draft Recommendation) and the Federal Trade Commission's Staff Report (FTC Guidelines) offer insights about what consumer privacy issues need to be addressed to adequately protect consumers. 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 industry. Both the Draft Recommendation and FTC Guidelines are useful starting points for the work needed to craft adequate consumer privacy protections to address consumer profiling by behavioural advertisers. This work should include examining the adequacy of industry self-regulatory codes adopted by companies in the EU and the U.S. to see how well these industry codes protect consumers' privacy. Available privacy-enhancing technologies also need to be examined to see if they help fill the privacy gaps. If industry self-regulation and privacy-enhancing technologies still expose consumers' privacy in the context of profiling by behavioural advertisers, new privacy and data protections for consumers need to be provided through new legislation, stronger industry self-regulation, privacy-enhancing technologies or some combination of the three.

The discussion of how to adequately protect mobile customers' information privacy in the context of profiling by behavioural advertisers will be continued in the second article in this series on Profiling the Mobile Customer that will appear in the next volume of the *CLSR*.

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 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.