Elsevier Editorial System(tm) for Computer Law & Security Report
Manuscript Draft

Manuscript Number: CLSR-D-08-00038

Title: Regulating mobile advertising in the European Union and the United States

Article Type: Full Length Article

Keywords:

Corresponding Author: Ms Evelyne Beatrix Cleff,

Corresponding Author's Institution: Law

First Author: Evelyne Beatrix Cleff

Order of Authors: Evelyne Beatrix Cleff

Abstract: XXXX

PUBLISHING AGREEMENT

THE COMPUTER LAW AND SECURITY REPORT (CLSR)

[Name of Licensor]
[Address]

hereby grants to **ELSEVIER SCIENCE Ltd.**,
PO Box 150 Kidlington Oxford OX5 1AS

a **non-exclusive licence** to publish the material identified below ("the material"):

until further notice a perpetual licence covering all future submissions to CLSR

and the non-exclusive right to include the material in all media including electronic and microfilm and to use the material in conjunction with computer-based electronic information retrieval systems, to grant permissions for photocopying, reproductions and reprints from *CLSR*, and to authorize document delivery and abstracting and indexing services, provided that any such copy reproduces the AUTHOR's and the Licensor's name and, if inserted by the Licensor, the appropriate copyright notice to run in conjunction with the copyright notice representing the publisher's limited rights.

The LICENSOR retains all residual Intellectual Property rights in the material and the AUTHOR asserts his/her right to be identified as the author of the material.

In the event that the material is first published in *CLSR*, unless agreed otherwise with the Editor, it is agreed that any re-publication of the material may include reference to its having first been published in *CLSR*.

The Licensor warrants that, as far as it is aware, the material does not and/or will not contain libellous or other unlawful statements, and does and/or will not infringe the intellectual property rights of others. If excerpts from copyrighted works requiring permission are included in the material, it is understood that by agreement with the Editor for the time being of CLSR the AUTHOR has obtained or will obtain written permission from the copyright owners and will credit the sources in the article.

The licensor also confirms that he/she has read and accepts the "Ethics in Publishing – Instructions to Authors note" below as published on the Elsevier Editorial System

Signed:

[This licence can be 'signed' and returned to Stephen Saxby by email confirming acceptance of its terms]

Date:

When completed please return this form to the Editor, Stephen Saxby, School of Law, The

University, Southampton SO17 1BJ, UK, E-mail: s.j.saxby@soton.ac.uk; Tel/Voicemail: +44 (0) 23 8059 3404 or fax +44 (0) 23 8059 3024

Ethics in Publishing: Instructions to Authors

This general statement will be supplemented by instructions to authors (as well as in communications to editors and peer reviewers) relevant for each journal.

Ethics and Procedures

General

The editor(s) and publisher of this Journal believe that there are fundamental principles underlying scholarly or professional publishing. While this may not amount to a formal "code of conduct", these fundamental principles with respect to the authors' paper are that the paper should:

- be the authors' own original work, which has not been previously published elsewhere
- reflect the authors' own research and analysis and do so in a truthful and complete manner,
- properly credit the meaningful contributions of co-authors and co-researchers,
- not be submitted to more than one journal for consideration (ensuring it is not under redundant simultaneous peer review), and
- be appropriately placed in the context of prior and existing research.

For a full description of the standards of expected ethical behaviour by all parties involved in the publishing process (the author, the journal editor, the peer reviewer, the publisher and the society for society-owned or sponsored journals) please see: http://www.elsevier.com/wps/find/intro.cws_home/publishing.

Of equal importance are ethical guidelines dealing with research methods and research funding, including issues dealing with informed consent, research subject privacy rights, conflicts of interest, and sources of funding.

While it may not be possible to draft a "code" that applies adequately to all instances and circumstances, we believe it useful to outline our expectations of authors and procedures that the Journal will employ in the event of questions concerning author conduct. Relevant conflicts of interest should be disclosed (see <http://www.elsevier.com/wps/find/authorshome.authors/conflictsofinterest>).

Last revised: 9 January 2007

Mobile advertising regulation

Regulating mobile advertising in the European Union and the United States

Evelyne Beatrix Cleff

College of Business - Oregon State University (USA) Affiliate Faculty: Aarhus School of Business,
Aarhus University (Denmark)

ABSTRACT

Mobile advertising is a gradually developing component of the marketing mix that includes advertisements directed to or accessed on consumers' mobile devices. Growing concerns about the protection of the consumers' personal data are being raised since mobile advertising may become an extremely intrusive practice in an intimate personal space. Approaches of protecting the consumers' personal information differ greatly throughout the world. This article contrasts the regulatory environment in the European Union and in the United States applicable to the consumer's privacy and personal data used for mobile advertising purposes while also examining the effectiveness of each of these approaches.

© 2008 Evelyne Beatrix Cleff. Published by Elsevier Ltd. All rights reserved.

1. Introduction

The introduction of ubiquitous wireless access through wide-area networks (e.g., 2.5 and 3rd generation mobile telephony), local area networks (e.g., wireless LAN), and proximity networks (e.g., Bluetooth) allows mobile device users to access Internet services and other server-based applications from mobile devices, and provides the means for location-based and personalized mobile advertising (m-advertising). Mobile devices equipped with Global Positioning Systems (GPS) are already on the market and soon radio frequency identification (RFID)¹ devices will be available. However, this exploitation will indirectly result in mobile devices becoming a vast storage area for personal information on consumers. This is because the consolidation of these technologies will simplify to electronically track the geographic location and Web surfing behavior of mobile device users.

Whether legislations applying to such practices are effective or useful is an open question. Different legal regimes regulating the use of personal information have been emerged. Among them are two dominant models, reflecting different approaches to the control of personal information.² First, the European Union (EU) mandates a comprehensive omnibus legislative approach that imposes significant restrictions on most data collecting and processing activities, not only within the borders of the Union but throughout the world if the data originates in a Member State. Second, the United States (U.S.), in turn, strives for a more market driven approach and regulates only extensive government processing of data.

The EU and the U.S. are each other's largest trading partners, and they also form the largest bilateral trade relationship in the world.³ Moreover, personal information processed for m-advertising purposes may be inherently global. Data can easily be transferred throughout the world and it is almost impossible to block

¹ For a detailed description of RFID systems see Hildner (2006) at pp. 134-135.

² Cate (1999), p. 179.

³ European Commission (September 2007): EU and the World - External Trade: *Bilateral Trade Relations*. Retrieved 23.04.2008 from http://ec.europa.eu/trade/issues/bilateral/countries/usa/index_en.htm and also European Commission (27.04.2007): *Facts and Figures on the European Union and the United States*. Retrieved 23.04.2008 from <http://www.eurunion.org/profile/facts.htm>.

data thorough either legal or technical means. In the case of the EU and the U.S. the legal approaches differ most sharply on how they value fair information practices.⁴ Under EU law, data protection is treated as a fundamental right and legislations in this field try to balance the interests of individuals with the legitimate need of businesses to gain value from customer data.⁵ In the U.S., the government is constitutionally limited from interfering in the private sector, particularly when expression is involved.⁶ Consequently the system places less value on the protection of personal information.

The purpose of this article is to contrast these two major approaches to the protection of personal data and legislation applying to sending of m-advertising. The question is whether there exist sufficient mechanisms to protect consumers' personal data, including the protection of their personal data, against unsolicited m-advertising messages (also known as SPAM) and unwanted uses or disclosure of that information. The exposure to another legal system (here that in the U.S.) is also helpful to realize the variety of possible approaches to find effective or useful solutions. The structure is as follows: part 2 contrasts the two regulatory philosophies in terms of fair information practices, and part 3 highlights the EU and U.S. framework applying to the processing of personal data for the purpose of m-advertising. Finally the article concludes with a discussion in part 4 that highlights the weaknesses of both systems in terms of protecting consumers' privacy and data protection in m-advertising.

1.1. Terminology and delimitation

Defining *privacy* is a dizzying issue and over the decades many attempts to define privacy have been made. It has proven to be quite complicated and difficult to define precisely what privacy is and the problem appears to be that privacy is an extremely broad concept.⁷ Moreover, a general attempt to compare U.S. legislation in terms of EU data protection would not be meaningful. This is because the European approach to data protection is fundamentally different than the U.S. approach. The EU legal framework defines *data protection* as the fair treatment of information about individuals and the legal system consists of rules that structure the collection and use of personal information. In the U.S. the term data protection may refer to concepts of data security or intellectual property principles such as copyright and trade secrets.⁸ In general, however, the concept of data privacy in U.S. law embraces data protection in the EU sense of the word.

In this article, concern is *information privacy* that is "*the right to control information about oneself*"⁹ and *physical privacy* that is "*the degree to which a person is physically accessible to others.*"¹⁰ Consumers should be able to determine for themselves the circumstances and extent that information about them is collected, used, and processed and should also have control over received advertising messages because unsolicited advertising can become an extremely intrusive practice in an intimate personal space. In the continuation of the above, the terms *fair information practices* and *data protection* will be used instead of *privacy* here and they will be used interchangeably. This is because the terms are more precise than the different usages of *privacy* and because developments within this area shall be placed in an international context.

In order to make a meaningful comparison between U.S. and EU regulation of fair information practices, the two standards must be understood. Chapter 2 will therefore deal with the regulatory philosophies of fair information practices within the two approaches.

To simplify the analysis, the focus of data protection lies on the commercial rather than the governmental sphere. The discussion of the U.S. approach is restricted to those at the federal level. This is due to the fact

⁴ Whitman (2004), pp. 1161-62.

⁵ See, for example, Data Protection Directive 95/46/EC, Article 1.

⁶ Cate (1999), p. 179.

⁷ See Solove, et al. (2005), pp. 40-44, analyzing the definition and the value of privacy in order to develop a theory of privacy and justifications for its legal protection. See also Kang (1998), providing a general primer on cyberspace privacy and a clarifying structure of philosophical and technological terms, descriptions and concepts of privacy.

⁸ Schwartz and Reidenberg (1996), p. 5.

⁹ Westin (1967), p. 2.

¹⁰ Joinson and Paine (2007).

that state laws are limited in their jurisdiction which precludes them from comparing to EU Directives.¹¹ In this article only the use of consumer data for m-advertising purposes is addressed. Only m-advertising sent to mobile devices are considered while voice telephony, pop ups, and banner advertising are excluded from the underlying analysis. Finally, detailed examination of all EU and U.S. legislations and regulation is beyond the scope of this article, but the most important are highlighted in the following sections.

2. Fair information practices: the regulatory philosophy

As mentioned before the approaches to regulate personal information differ greatly between the “*closely kindred*” societies of the EU and the U.S.¹² Especially how the two approaches value personal data differs: whereas the EU approach promotes a right to respect personal dignity, the U.S. approach is oriented towards value of liberties, and especially liberty of persons (including businesses) against the state.

2.1. European Union

Article 8 of the European Convention of Human Rights (ECHR) protects “*the right to respect for private and family life,*” and the Charter of Fundamental Rights of the European Union¹³ (hereafter, the Charter) features articles on both “*Respect for Private and Family Life*” and “*Protection of Personal Data.*” This philosophy is reflected in the data protection law of the EU. Article 1 of the Data Protection Directive¹⁴ requires Member States to “*protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data.*” Information privacy is therefore on par with the rights of self-determination, freedom of thought, and freedom of expression.

However, the protection of personal data prevails and Article 9 of the Directive itself states that Member States are permitted to make exceptions “*for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression,*” but only with regard to two of the Directive’s substantial chapters. Member States may define exemptions or derogations from both the prohibition on processing sensitive data, and the requirement of notification of information processing activities for data processing for “journalistic” and “literary” purposes. Since there is no reference to the other substantive rights (i.e. non-journalistic and non-artistic, or commercial expression is not in any way accommodated by the Directive) from the article permitting exceptions for expressive undertakings, it is clear that the protection of personal data takes precedence over others’ rights to freedom of expression and the press.¹⁵

On the one hand, advertising as a form of communication is protected by the freedom of expression stated in the European Convention on Human Rights (ECHR).¹⁶ On the other hand advertising is a service and therefore also protected as one of the four freedoms protected by Treaty on the European Union, namely the freedom to provide services. However, in both cases restrictive legislations may be adopted under certain conditions:

¹¹ It is of course possible to compare State consumer protection laws with EU Directives transposed into national law. Often these laws are more protective of consumers’ personal data.

¹² Whitman (2004), p. 1151.

¹³ The Charter was *proclaimed* in 2000, but not made legally binding, by the European Council. The Charter focuses on dignity, freedoms, equality, solidarity, citizens’ right, and justice as its fundamental values. The Charter’s relationship to the ECHR is intended to be consistent, but allowing for higher levels of protection.

¹⁴ Directive 95/46/EC.

¹⁵ Cate (1999), pp. 225-26.

¹⁶ ECHR, Article 10(1) states that: “*Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.*”

In terms of freedom of expression, the ECHR states that restrictive legislation may be necessary in a democratic society¹⁷ and the European Court of Human Rights has held that “*freedom of expression constitutes one of the essential foundations of ... a society, one of the basic conditions for its progress and for the development of every man. Subject to Article 10(2), it is applicable not only to ‘information’ or ‘ideas’ that are favorably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no ‘democratic society’*”.¹⁸

With regard to the freedom of services, restrictive EC legislations regulating advertising may be adopted, when it serves to protect the public interest, is not disproportionate to the intended objective,¹⁹ and does not go beyond what is necessary to achieve that objective.²⁰ The ECJ has held that the protection of consumers represents an imperative reason of public interest justifying restrictions on the freedom to provide services.²¹ Consumer protection is included in Article 153 and 95 of the Treaty, which promote the interests, health and safety of European Consumers. Such policies are designed in order to ensure that the internal market is open, fair, and transparent, allowing consumers to exercise real choice and a right to information. These requirements are also reflected in legislations on advertising and data protection, as they include certain information and transparency requirements to ensure consumer confidence and fair trading. These legislations will be analyzed in the next section.

Basically, the EU strives for a protection of a right to respect personal dignity which is seen to be the first of the ‘indivisible, universal values’ (human dignity, freedom, equality, solidarity), that the Union is founded on.²² Also the European Court of Justice (ECJ) has acknowledged human dignity as an object principle of Community law: “*It is for the Court of Justice, in its review of the compatibility of acts of the institutions with the general principles of Community law, to ensure that the fundamental right to human dignity and integrity is observed.*”²³ Therefore, this fundamental value influences the other fundamental rights recognized by EU law. This is also reflected in legislations applying to data protection, and all instances of data collection, use, and sharing throughout the society are covered establishing thereby a “*right to privacy*” for consumers in commercial transactions.²⁴

In Europe, Member States take an active role in the implementation of fair information practices for personal information and the Data Protection Directive designates national data protection authorities as being responsible for data-related activities. Compared to Americans, European citizens accept intensive government involvement in their daily lives.²⁵ European governments are normally the guarantors of citizens’ rights and entitlements and this has been interpreted to include protecting individuals from interference with their legal rights by other individuals or businesses.²⁶ From this it follows that, in the EU, there is an acceptance of more extensive government involvement in regulating citizens’ communications and the flow of information.

¹⁷ Ibid., Article 10(2): “*The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.*”

¹⁸ ECHR, *Handyside v. United Kingdom* (Appl. No. 5493/72), Ser. A, No. 24, para. 49 and ECHR, *Sunday Times v. the United Kingdom* (Appl. No. 6538/74), Ser. A, No. 30, para. 64.

¹⁹ ECJ, C-352/85, para 36.

²⁰ ECJ, C-390/99, para. 33.

²¹ See, for example, ECJ, C-288/89, para. 14.

²² Commentary of the Charter of Fundamental Rights of the European Union, p. 23, commenting on Article 1 (of the Charter) on Human dignity, a right that is inviolable and must be respected and protected.

²³ ECJ, C-377/98, para. 70 .

²⁴ Smith (2001), p. 9.

²⁵ Whitman (2004), p. 1156.

²⁶ Directive 95/46/EC, Article 28.

2.2. United States

Freedom of speech and freedom of expression are guaranteed in the First Amendment to the U.S. Constitution and are among the freedoms most valued by Americans.²⁷ This protection imposes limits of the government's ability to regulate the flow of information, especially with regard to personal data.

The Constitution affords, however, "*lesser protection to commercial speech than to other constitutionally guaranteed expression.*"²⁸ Advertising is an example of commercial expression protected by the First Amendment, however it may, for example, be regulated if it is found to be *deceptive*. Content regulation of advertising or *commercial speech*²⁹ is considered to be appropriate in order to prevent communication of false, deceptive, or misleading information.³⁰ Otherwise, advertising may only be regulated if the regulation passes a three-part test set out in court cases.³¹

Unlike the broad coverage of data protection law in the EU, data protection regulation in the U.S. is fragmented, and narrowly targeted to regulate specific industry sectors and consumer protection concerns. This is because federal U.S. laws focus on privacy rights to individuals in a commercial context and generally address situations where the free market has failed to adequately protect consumers' privacy and/or personal data. The market-based, self-regulatory approach is based on the prevailing attitude that the protection of personal data is an economic issue or a matter of consumer protection, rather than related to protecting individuals' fundamental rights.³²

There are four features of American society and system of government that are decisive for this regulatory approach: First, American values are much more orientated toward values of liberty, and most importantly liberty against the state. Therefore, the right to freedom from intrusion by the state, especially in one's home, is prioritized.³³ Businesses are considered persons under the law in the U.S., so businesses, as well as natural persons, have constitutional rights against excessive government regulation.³⁴ To a certain extent, the U.S. approach towards fair information practices reflects the citizen's distrust of a centralized government. Therefore, citizens generally have much greater protection against the collection and use of personal information by government, than by the private sector.³⁵ Second, the unrestricted flow of information is seen to be essential for a democratic society and market economy. The importance of open data flows is also reflected in the U.S. Constitution, for example, in the provisions for freedom of expression.³⁶ Third, the preference for private actions restrains the government from unnecessarily interfering with private action. Thus, market-based approach based on industry self-regulation is favored in the U.S. Finally, the U.S. has adopted a system to keep markets open which limits governmental interference. This does not mean that the government does not play a role in protecting personal information at all, but the legal framework in the private sector is largely limited to facilitating individual action and often aimed at protecting vulnerable populations, such as children, or sensitive data, such as financial data, or health information. Moreover, firms

²⁷ Tsai (2004), p. 86.

²⁸ *U.S. v. Edge Broadcasting*, 509 U.S. 418, 426 (1993) (quoting *Board of Trustees of State Univ. of N.Y. v. Fox*, 492 U.S. 469, 456 (1989)).

²⁹ Advertising is considered to be a form of '*commercial speech*' which refers to "*expression related solely to the economic interests of the speaker*" and "*speech proposing a commercial transaction*". See Boedecker, et al. (1995), p. 38 (analyzing the application of First Amendment law to various forms of commercial expression, and the current standard used by courts to identify commercial speech).

³⁰ See *R.A.V. v. City of St. Paul*, 505 U.S. 377 (1992).

³¹ First, the regulation must reflect that the government has a substantial interest in regulating the business practice. Second, the government's position must be directly advanced by the regulation. Third, the regulation must not be more extensive than necessary to advance the interest (*Central Hudson Gas & Electric Corp. v. Public Service Commission*, 447 U.S. 557, 591 (1980)).

³² Barnes (2006), p. 175.

³³ Whitman (2004), p. 1156, quoting Rozen (2000), who examines the legitimate needs of law enforcement and the demands of individual privacy.

³⁴ U.S. Constitution Fifth Amendment: Due Process Clause that provides procedural and substantive due process rights.

³⁵ Shaffer (1999), p. 422.

³⁶ U.S. Constitution, Art. I, §8.

that process personal data argue that restrictions imposed on collection, use, and transfer of personal information would conflict with the established property rights and would infringe on the processors' freedom of speech.³⁷

The Supreme Court has never created an absolute right on the treatment of personal data.³⁸ The Court has, however, outlined an “*expectation of privacy*” resulting from the Fourth Amendment, but that expectation is not guaranteed when a consumer discloses data to a third party.³⁹ In line with this view of fair information practices, the U.S. approach to data protection is relatively piecemeal, containing sector-specific legislation and regulation. However, the U.S. framework for fair information practices is an emerging topic: laws have been implemented in cases where there has been shown to be a market failure justifying the adoption of consumer privacy regulation. There are numerous federal statutes that set data protection standards for specific industry sectors and this is supplemented by more protective consumer protection law at the state law level. Further, administrative agencies that have been given power by Congress to adopt legislative rules under enabling statutes passed by Congress play an active role in regulating business practices to protect consumers from unfair or deceptive business practices, including advertising practices.

The overriding philosophy has been to resist the introduction of comprehensive legislative protection of personal information on the grounds that the market will self-regulate through compliance with code of conducts.⁴⁰ This approach can be found in the *Framework for Global Electronic Commerce* which considers data protection critically important but “*private efforts of industry working in cooperation with consumer groups are preferable to government regulation [...]*.”⁴¹

To a certain extent, this difference in the constitutional role of government between the EU and the US is lessened by the broad constitutional authority given to the federal government in the U.S. to adopt legislation that regulates business practices concerning interstate (between the states) and foreign commerce, including consumer protection legislation. Given the broad scope of business practices that are considered to be in interstate commerce, for example use of the telephone or Internet in conducting business, the U.S. government has extensive power to regulate m-advertising practices as long as it doesn't violate the constitutional rights of those businesses.

3. Regulation of fair information practices

While the U.S. is restricted by its federal Constitution, especially due to the guarantee of speech stated in the First Amendment, which makes preventive legislation in terms of fair information practices more difficult because it provides an avenue for businesses to challenge such legislation as violations of commercial free speech rights, there is more flexibility for European lawmakers to create uniform legislations on data protection. With regard to m-personalized and location-based advertising, service providers may need to collect personal and location data. Mobile users are therefore confronted with two issues, namely 1) the processing of the mobile user's personal data and 2) the generation of unsolicited m-advertising.⁴²

3.1. The EU approach

The EU regulatory framework applying to information society service includes mobile and wireless communications.⁴³ EU legislations refer to advertising as *commercial communication* which is defined as “*any form of communication designed to promote, directly or indirectly, the goods, services or image of a*

³⁷ See Cohen (2000), p. 1375.

³⁸ For an extensive discussion of case law upon which fair information practices is regulated in the U.S. has been based, see Cate (1999), pp. 196-209.

³⁹ See *U.S. v. Hambrick*, 55 F. Supp. 2d 504, 506 (1999).

⁴⁰ Blanchette and Johnson (2002), p. 39.

⁴¹ Clinton and Gore (01.07.1997): Framework for Global Electronic Commerce. Retrieved 15.04.2008 from <http://isis.ku.dk/kurser/blob.aspx?feltid=196532>.

⁴² Gratton (2002), p. 64.

⁴³ European Commission (December 2007): Information Society: *In brief*. Retrieved 03.04.2008 from http://europa.eu/pol/infso/overview_en.htm.

company, organization or person pursuing a commercial, industrial or craft activity or exercising a regulated profession.”⁴⁴ Consequently m-advertising is considered to be an electronic commercial communication as it is delivered by *electronic mail*.⁴⁵ Policies aim to encourage competition in this area, to improve the functioning of the internal market, and to guarantee basic consumer interests that would not be guaranteed by market forces. The framework is intended to provide a set of rules that are technology neutral and flexible enough to deal with fast changing markets in the electronic communication sector.⁴⁶

As analyzed above, the EU has less stringent freedom of speech protections than the U.S. and is therefore more flexible in creating a legal framework of fair information practices. In *von Hannover v. Germany* the European Court of Human Rights has moved towards greater protection of personal rights and argued that the freedom of expression is fundamental to any democratic society as long as the media does not transgress their limits, particularly not on the account of the rights of others. By the opinion of the Court, Article 10 of the ECHR needs to be interpreted in a limited sense.⁴⁷

EU legislations in this area outline basic principles for both data protection and the free movement of such data. The legal framework intends to create series of fair information practices that define obligations and responsibilities applicable to the processing of personal information and the sending of m-advertising. Moreover, legislations applying to fair information practices are characterized by an overarching structure that addresses, in general terms, all the instances of the processing of personal data. Therefore, this section is subdivided into two parts: the first part highlights data protection rules regarding m-advertising and the second part presents the requirements that have to be met when sending m-advertising to consumers.

3.1.1. Data protection rules regarding m-advertising

The EU legislations on data protection are in line with the guidelines developed by the Organization for Economic Cooperation and Development (OECD).⁴⁸ Several Directives have been introduced that relate to the processing of personal data in general, the processing of personal data in the communication sector, and legislations regarding the obligation for data retention.

The Data Protection Directive applies when there is a *processing*⁴⁹ of *personal data*⁵⁰ and sets strict restrictions on how personal data can be collected and used as well as it requires that each Member State

⁴⁴ Directive 2000/31/EC, Article 2(f).

⁴⁵ Directive 2002/58/EC, Article 2(h): *electronic mail* is defined as “any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient”.

⁴⁶ European Commission (March 2007): *Mobile and Wireless Communications, Relevant Policies: Mobile & Wireless Communications: Lowering Costs, Stimulating Growth*. Retrieved 28.03.2008 from http://ec.europa.eu/information_society/industry/comms/mobile/pol/index_en.htm.

⁴⁷ ECHR, *von Hannover v. Germany* (Appl. No. 59320/00), para. 45. According to the Court, privacy also includes elements of personal identity (e.g. name and image) as well as human physical and mental integrity which ensures that individuals can develop their own personal relationships with others without external influence.

⁴⁸ OECD: *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (from 23 September 1980). Retrieved 14.03.2008 from http://www.oecd.org/document/18/0,3343,es_2649_34255_1815186_1_1_1_1,00.html.

⁴⁹ Directive 95/46/EC, Article 2(b): The definition of *processing* given in the Directive is very broad in scope as it covers “any operation or set of operations” whether or not automated, including the “collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.”

⁵⁰ *Ibid.*, Article 2(a): What is considered to be *personal data* is also defined very broadly as “any information relating to an identified or identifiable natural person.” There are basically no limits on content or technology and therefore not only textual information are included, such as name, address, phone number, email, etc., but also photographs, audiovisual images, and sound recordings of an identified or identifiable person. The Article 29 Working Party has prepared a document with explanations on the scope of the term *personal data* which was seen to be necessary since national laws implementing the Directive show different interpretations to this concept. See Article 29 Working Party (2007).

implements an independent national authority responsible for the protection of these data.⁵¹ Basically, the Data Protection Directive aims to protect the processing of data by placing guidelines determining when such processing is lawful. The provisions are related to the quality of the data and the legitimacy of data processing.⁵² Even though the Directive was implemented before specific problems arose related to providing information society services, it does apply to new technologies and business methods because “*the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention.*”⁵³

Another legislation including provisions regarding data protection is the E-Privacy Directive.⁵⁴ This Directive can be considered to be a sector-specific directive within the area of data protection as it translates the principles set out in the Data Protection Directive into specific rules for the electronic communication sector. The Data Protection Directive is viewed as the *lex generalis* which is applicable to the processing of personal data unless a *lex specialis* determines otherwise.⁵⁵ The E-Privacy Directive can be viewed as such a *lex specialis*.

Member States shall protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data. It requires amongst others, that Member States must ensure the confidentiality of communications made over public communication networks and the personal data that is carried on it. According to Article 1(1) the Directive “*harmonizes the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communications sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.*” In addition, Article 2 states that the definitions of the Data Protection Directive shall apply. However, more specific personal data which are of importance to location-based-services, such as traffic⁵⁶ and location data⁵⁷ are included in the E-Privacy Directive. The Directive differentiates between personal, location, and traffic data but a distinction is not always easy to make as many kinds of combinations are possible, for example, personal data may also be location data.⁵⁸

As far as personal data are concerned, the Data Protection Directive requires, with respect to each and every instance of data processing, that the processor proves that the processing is lawful.⁵⁹ Where data collection is permitted, the Directive imposes extensive restrictions on personal data processing, grants individual rights to *data subjects*, and defines specific procedural obligations, such as notification to national authorities. EU

⁵¹ Directive 95/46/EC, Article 28.

⁵² For more information about the Data Protection Directive, please see SCADPlus (31.08.2007): Information Society: Protection of personal data. Retrieved 09.04.2008 from <http://europa.eu/scadplus/leg/en/lvb/l14012.htm>. This website gives a nice overview of the Directive and summarizes also other legislations applicable to data protection.

⁵³ Directive 95/46/EC, Recital 27.

⁵⁴ Directive 2002/58/EC. This Directive has been amended by Directive 2006/24/EC on issues related to data retention for the purpose of investigating, detecting and prosecuting infringements. Moreover, the European Commission has introduced a Proposal for a Directive (COM(2007) 698 final on consumer protection cooperation) amending the E-Privacy Directive in particular on issues on security and enforcement provisions.

⁵⁵ The principle of *lex specialis* is for example explained in Nielsen and Tvarnø (2005), pp. 206-07.

⁵⁶ Directive 2002/58/EC, Article 2(b): *traffic data* is defined as “any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof”

⁵⁷ Ibid., Article 2(c): *location data* means “any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.”

⁵⁸ At the beginning and at the end of a communication with a mobile device, traffic data include information about the geographical position of the device, and such traffic data are therefore location data. Location data which is needed for the purpose of the realization of a communication are traffic data.

⁵⁹ This approach restricts liberty to a much greater extent than a regime that requires that the government prove that the data processor has violated the law.

data protection laws impose requirements on all sectors of industry and apply to personal data processed by conventional or automatic means.⁶⁰

Rather than prohibiting or restricting harmful uses of personal information and permitting all other uses, the Data Protection Directive starts from the opposite direction and prohibits all uses, except under certain conditions. Consequently, personal data may only be processed in certain specific situations laid down in the Directive.⁶¹ Personal data may be collected only for “*specific and legitimate purposes*,” may not be “*excessive*,” and the processing must be “*lawful and fair*.”⁶² Provisions regarding the processing of so-called *sensitive data* (e.g. race, religion, and health) are even more stringent.

A general principle is that personal data may only be processed for the purpose of m-advertising when the consumer has been informed about the data processing and has explicitly given his/her consent.⁶³ Notification to the consumer include information about the processors address, the type of data which will be processed, the purpose and duration of the processing, the existence of the right to access, delete and/or correct his/her personal data, and whether the data will be transferred to a third party for the purpose of providing m-advertising.⁶⁴ Moreover, the individual must be given the right to object at any time on legitimate grounds to the processing of personal data as well as the right to disallow the use of their personal information for marketing purposes.⁶⁵ With respect to security, the data processor is required to take measures appropriate to the risks involved to protect the security of data processing and transmission. This applies not only to the protection of personal data from “*accidental or unlawful destruction or accidental lost*,” but also to provisions prohibiting “*unauthorized alteration or disclosure or any other unauthorized form of processing*.”⁶⁶ Subject to limited exceptions, transfer of personal data to non-EU Member States which are considered to offer an “*inadequate*” level of data protection is prohibited.⁶⁷

If *traffic and location data* can be considered to be personal data, the general rules laid down in the Data Protection Directive apply otherwise the specific provisions of the E-Privacy Directive must be taken into consideration:

For location data that are not personal data, e.g. relating to telecommunications subscriptions by legal persons, only the E-Privacy Directive applies. Article 9 states that location data other than traffic data “*relating to users or subscribers of public communications networks or publicly available electronic communications services*”, may only be processed if the data are made anonymous, or with the consent of the mobile user receiving m-advertising services. Users must also be able to express their refusal to have their movements traced by their network providers. Basically, a data processor may only use location data if there is a value added service, e.g. location-based m-advertising that cannot be provided without this processing. In addition, the processing has to be limited to the duration necessary to provide this service. Unnecessary processing is generally prohibited, unless the derogation of Article 15 applies to the situation.⁶⁸

Article 5 of the E-Privacy Directive states that the in essence the communications and related traffic data by means of a public communication network and publicly available electronic communications services are

⁶⁰ Directive 95/46/EC, Recital 27.

⁶¹ Ibid., Articles 8(4) and (5), and 13: Member States may adopt exemptions that serve public interests such as public security, the investigation of crimes, etc.

⁶² Ibid., Article 6.

⁶³ Ibid., Article 7(a). See also Cleff (2007), pp. 267-68.

⁶⁴ See Ibid., Article 10.

⁶⁵ Ibid., Article 14.

⁶⁶ Ibid., Article 17(1).

⁶⁷ Ibid., Articles 25 and 26.

⁶⁸ Article 15 of Directive 2002/58/EC states that Member States may adopt legislative measures “*when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system.*”

confidential. In particular, listening, tapping, storage or other kinds of interception or surveillance of communications by persons other than users, is prohibited without the consent of the users concerned, unless processing is subject to the derogations of Article 15. The Data Retention Directive⁶⁹ regulates the mandatory storage of traffic data. The Directive requires that service and network providers keep records of customers' communications for up to two years in order to ensure that the data are available *"for the purpose of investigation, detection and prosecution of serious crime, as defined by each Member State in its national law."*⁷⁰ The requirements only concern traffic data and not the content of the message, such as the date, destination, duration of communications, and location of mobile communication equipment. To traffic data not listed in Article 5 of the Data Retention Directive the provisions of the E-Privacy Directive continue to apply. Such traffic data, e.g. the consumer's search behavior, must be erased or made anonymous as soon as they are no longer needed for the purpose of m-advertising.⁷¹ Certain general conditions apply to the processing of traffic data for m-advertising purposes: the duration of the processing must be restricted to what is necessary to perform m-advertising; the consumer must be informed of the types of traffic data used and of the duration of the processing; and the processing is only permitted by persons *"acting under the authority of providers of the public communications networks and publicly available electronic communications services."*⁷²

3.1.2. Requirements to meet when sending m-advertising

Transparency is a core requirement of EU law that also applies to m-advertising and which is necessary to protect consumers against unfair commercial practices (that is dishonest and negligent conduct). Sending advertising messages to mobile devices could mislead consumers if adequate information about the product or service is not provided. Certain claims made in m-advertising require the advertiser to provide additional information to the consumer about the terms and conditions of the advertising in order to prevent misinterpretation. In addition to the information requirements concerning the processing of personal data, further provisions apply to the sending of m-advertising messages. Therefore, messages sent to mobile devices must at least satisfy the following conditions:

In the EU, the opt-in mechanism applies for all business-to-consumer (B2C) commercial communications.⁷³ Therefore, the mobile user must also give his/her consent prior to the sending of such messages. There is a limited exception to this rule for messages sent to existing customers by the same sender on its similar services or products.⁷⁴ If such an existing customer relationship exists, the service provider who obtained the data from its customer may use them for the marketing of similar services or products. The mobile user must be offered the right to object *"free of charge and in an easy manner"*,⁷⁵ and also each subsequent message should include an easy way to object from further commercial communications (opt-out). False identifiers return numbers, or addresses are prohibited.

The Distance Selling Directive and the E-Commerce Directive requires advertisers to provide comprehensive information: Some requirements are overlapping as both Directives require providing consumers with information such as name, valid return address and/or cell phone number. In addition the Distance Selling

⁶⁹ Directive 2006/24/EC. This Directive must be implemented by the Member States in national law by 15 September 2009.

⁷⁰ Ibid., Article 1(1).

⁷¹ Directive 2002/58/EC, Article 6(1).

⁷² Ibid., Article 6(3)-(5).

⁷³ Ibid. Article 13(1): As a general rule, *commercial communications* must comply with the rules applicable to them in the Member States. In cases where natural persons are not protected under Directive 2002/58/EC (e.g. when a natural person is not a subscriber), against unsolicited commercial communications, Member States must also ensure under the E-Commerce Directive that service providers undertaking unsolicited commercial communications by electronic mail, consult regularly and respect the opt-out registers in which natural persons not wishing to receive such messages can register themselves (Directive 2000/31/EC, Article 7)

⁷⁴ Directive 2002/58/EC, Article 13(2).

⁷⁵ Ibid., however, the *"costs for the transmission of this refusal"* are not considered (Recital 41) and in the case of mobile communication, each time a mobile message is sent a fee is charged for the transmission.

Directive requires giving information about the main characteristics of the goods and services, the price of the goods or services including all taxes, the cost of using the means of distance communication, where it is calculated other than at the basic rate, the period for which the offer or the price remains valid, etc.⁷⁶ The E-Commerce Directive, in turn, requires certain information to be included in promotional offers, such as discounts, premiums, and gifts and competitions or games.⁷⁷ The information sent to the consumer must be made clear and shall be provided in a clear and comprehensible manner in any way appropriate to the means of distance communication used.⁷⁸ The consumer must be able to store the received information on a durable medium. Moreover, the Directive serves as a protection from unsolicited selling.⁷⁹

General content requirements must be considered when doing m-advertising: Mobile ads must be clearly identifiable as commercial communications, for example, by a clear indication in the ad containing *advertisement*.⁸⁰ It is illegal to disguise or conceal the identity of the sender on whose behalf the communication is made.⁸¹ Moreover, unfair commercial practices, including misleading and aggressive advertising, are prohibited throughout the EU.⁸²

3.2. The U.S. approach

Under U.S. law m-advertising falls under the concept of *commercial electronic mail message* which is “any electronic mail message having the primary purpose of commercial advertisement or promotion of a commercial product or service, including content on an Internet Web site operated for a commercial purpose.”⁸³ The legal framework on fair information practices is fragmented, ad hoc, and narrowly targeted to cover specific sectors and concerns. Federal legislation regulating SPAM and the use of unfair and deceptive business practice apply, in turn, to all business practices.

Additionally, in the U.S. telecommunication carriers are heavily regulated which results in some consumer protection and some of that protection provides personal data protection for subscribers of mobile carriers. Generally the direct marketing industry faces fewer restrictions in part due to constitutional free speech rights that include commercial expression, such as advertising.

There are two main federal administrative authorities which are in charge for the regulation of m-advertising. The Federal Trade Commission (FTC) has responsibility for enforcing and administering laws designed to protect consumers from unfair or deceptive practices.⁸⁴ The Federal Communications Commission (FCC) is in charge of regulating and enforcing statutes related to the processing of consumer data by telecommunication network providers, which includes mobile carriers.⁸⁵

This section will point out federal provisions restricting m-advertising practices that are unfair deceptive, or present an intrusion into the mobile users privacy.

⁷⁶ Directive 97/7/EC, Article 4(1).

⁷⁷ Directive 2000/31/EC, Article 6(c) and (d).

⁷⁸ Directive 97/7/EC, Article 4(2).

⁷⁹ Ibid., Article 5(1).

⁸⁰ Directive 2000/31/EC, Article 6(a).

⁸¹ Directive 2002/58/EC, Article 13(4).

⁸² Directive (2005/29/EC) includes rules and principles which give consumers the same protection against unfair practices whether they are buying from their corner shop or purchasing from a website based abroad.

⁸³ 15 U.S.C. § 7702(2).

⁸⁴ See Federal Trade Commission (29.03.2008): *About the Federal Trade Commission*. Retrieved 15.04.2008 from <http://ftc.gov/ftc/about.shtm>.

⁸⁵ See Federal Communications Commission (29.02.2008): *About the WTB*. Retrieved 15.04.2008 from <http://wireless.fcc.gov/index.htm?job=about>.

3.2.1. Unfair trade practices

The FTC is the primary federal consumer protection agency and administers and enforces the Federal Trade Commission Act (FTC Act),⁸⁶ which is the nation's most comprehensive federal statute to protect consumers from deceptive or unfair practices.⁸⁷ While applying to any medium, it prohibits false, unsubstantiated or deceptive advertising claims.⁸⁸ From this follows, that advertisers may not publicize false, unsubstantiated or deceptive advertising material or engage in unfair or deceptive practices.

Even though there are generally no particular information requirements, information provided by advertisers must be accurate and relevant information must not be left out (sometimes there are content requirements, for example to comply with spam and telemarketing rules). With respect to fair information practices, generally the FTC has encouraged businesses to self-regulate and individuals to be aware of the processing of their personal data. The FTC states on its homepage: "[...] as personal information becomes more accessible, each of us – companies associations, government agencies, and consumers – must take precautions to protect against the misuse of that information."⁸⁹ It is not required by law that businesses generate a privacy policy but if such a policy is promulgated, the business must comply with that policy or risks FTC enforcement action. This is line with Section 5 of the FTC Act that prohibits deceptive or unfair acts or practices and grants the FTC the authority to seek relief for violations.⁹⁰

Another federal statute dealing with deceptive advertising practices is the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)⁹¹ and applies to all commercial electronic messages including m-advertising.⁹² The provisions of the CAN-SPAM Act are supported by rules adopted by the FTC⁹³ and the FCC.⁹⁴

Basically the CAN-SPAM Act requires that businesses clearly label commercial electronic messages sent to electronic devices such as m-advertising, uses a truthful and relevant subject line, uses a legitimate return address, provides an opt-out option, and process opt-out requests within ten business days.⁹⁵ It is also prohibited to knowingly use third parties that send commercial communications to mobile users that violate

⁸⁶ 15 U.S.C. §§ 41-58 (2007). Moreover, Section 18 of the FTC Act states that the FTC has the power to implement trade regulation with the force and effect of law that "define with specificity" acts or practices that the FTC finds unfair or deceptive.

⁸⁷ A representation, omission, or practice is *deceptive* if it is likely to mislead consumers and affect consumers' behavior or decisions about the product or service (Policy statement on deception, appended to *Cliffdale Association*, 103 F.T.C. 110, 175 (1984)). Furthermore, an act or practice is *unfair* if the damage it causes is 1) substantial, 2) not outweighed by other benefits, and 3) not reasonably avoidable (Policy statement on deception, appended to *International Harvester*, 104 F.T.C. 949 (1984)).

⁸⁸ 15 U.S.C., §§ 41-58, Section 5.

⁸⁹ See Federal Trade Commission: Privacy Initiatives: *Introduction*. Retrieved 16.04.08 from <http://www.ftc.gov/privacy/>

⁹⁰ The FTC has used this authority to enforce privacy policies promulgated by businesses. See, for example, *FTC v. Toysmart*, File No. 00-11341-RGS (filed July 10, 2000), alleging that Toysmart, contrary to the terms of its privacy policy, disclosed personal customer information to third parties. See also, Agreement Containing Consent Order, *FTC v. Gateway Learning Corp.*, File No. 042-3047 (2003), accusing Gateway of renting user information collected on its Web site, in violation of its privacy policy. See also King (2008), p. 252.

⁹¹ 15 U.S.C. §§ 7701-7713 and 18 U.S.C. § 1037.

⁹² The CAN-SPAM Act defines in Section 3(2)(A) electronic messages as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)."

⁹³ 16 C.F.R. § 316. The purpose of these rules is to interpret the CAN-SPAM Act provisions and clarify the different type of electronic messages. See also Federal Trade Commission: SPAM: *for Consumers Page*. Retrieved 16.04.08 from <http://www.ftc.gov/bcp/conline/edcams/spam/consumer.htm>.

⁹⁴ FCC's Mobile Spam Regulations. See also Federal Communications Commission (01.05.2007): FCC Consumer Facts: CAN-SPAM: *Unwanted Text Messages and E-Mail on Wireless Phones and other Mobile Devices* Retrieved 16.04.08 from <http://www.fcc.gov/cgb/consumerfacts/canspam.html>.

⁹⁵ 15 U.S.C. § 7702, Section 5.

the CAN-SPAM Act.⁹⁶ However, transactional or relationship messages, or notices to facilitate a transaction the consumer has already agreed to are excluded from most of the information requirements.⁹⁷ These messages must be labeled with accurate header information but other CAN-SPAM requirements, such as the opt-out notice, do not apply.⁹⁸

3.2.2. Special FCC rules against unsolicited commercial communications

The FCC rules have been issued in order to prevent mobile devices from being overwhelmed with unsolicited commercial messages.⁹⁹ However, whether the *opt-in* or the *opt-out* mechanism applies depends on the specific transmission technique used to deliver m-advertising to mobile devices.

Electronic commercial messages, that use an *Internet address that includes a wireless Internet domain name* (usually the part of the address after the individual or electronic mailbox name and the “@” symbol), may not be sent to mobile devices without the consumers prior consent.¹⁰⁰ This type of message is categorized as *Mobile Service Commercial Message* (MSCM) which is defined as a “*commercial electronic mail message that is transmitted directly to a wireless device that is utilized by a subscriber of commercial mobile service (...) in connection with such service.*”¹⁰¹ The FCC has created a wireless domain name list containing the domain names used for mobile service messaging to enable advertisers to determine which addresses, containing those domain names, are directed at mobile devices.¹⁰² Without obtaining the advance consent of the recipient of a MSCM, it is prohibited to send any MSCM to addresses that have been listed on the official list for at least 30 days, or at any time if the sender knows that the message is being sent to a mobile device via a wireless Internet domain name.¹⁰³ SMS transmitted solely to phone numbers (as opposed to those sent to addresses with reference to Internet domains) and e-mail messages which have been forwarded by the mobile user to his/her own device are not covered by the FCC’s ban on sending unsolicited commercial electronic messages. However, the use of autodialers to make calls to mobile phone numbers, including phone-to-phone SMS and voice calls, are regulated by the Telephone Consumer Protection Act of 1991 (TCPA).¹⁰⁴ The Act prohibits the use of auto-dialling equipment to deliver m-advertising without prior consent of the consumer.¹⁰⁵

In line with the general framework of the CAN-SPAM Act, the FCC’s rules do not apply to transactional or relationship messages. It should be emphasized here that the FTC is responsible for determining the criteria for categorizing a message as primarily commercial and determining what types of messages are excluded as transactional or relationship messages. Charitable and political solicitations are not commercial electronic messages.

No matter which type of message is used for m-advertising the general FTC rules must be followed. This includes identification as a solicitation or advertisement, offering the possibility to reject future messages, and including a valid return address: Moreover m-advertising messages may not be false or deceptive.

⁹⁶ Ibid. § 7705, Section 6 (b).

⁹⁷ Ibid. § 7702, Section 3(17).

⁹⁸ 16 C.F.R. § 316.

⁹⁹ Section 14 of the CAN-SPAM Act states that the FCC shall issue rules to protect consumers from “*unwanted mobile service commercial messages.*”

¹⁰⁰ Federal Communications Commission (01.05.2007): FCC Consumer Facts: *CAN-SPAM: Unwanted Text Messages and E-Mail on Wireless Phones and other Mobile Devices* Retrieved 16.04.08 from <http://www.fcc.gov/cgb/consumerfacts/canspam.html>.

¹⁰¹ 15 U.S.C. §7701,

¹⁰² Moreover, the FCC requires that all Commercial Mobile Radio Service (CMRS) providers make all domain names used to offer mobile subscribers messaging for mobile devices available to the agency (47 C.F.R. § 64.3100(e)). Please refer also to Federal Communications Commission (01.10.2007): *Consumer Policy Issues, Can Spam, Unwanted Commercial Electronic Mail*. Retrieved 16.04.08 from <http://www.fcc.gov/cgb/policy/DomainNameDownload.html>.

¹⁰³ 47 C.F.R. § 64.3100(a)(4).

¹⁰⁴ 47 U.S.C. § 227.

¹⁰⁵ 2003 TCPA Order, para. 165.

3.2.3. Rules protecting customer information

The Telecommunication Act of 1996¹⁰⁶ and FCC rules¹⁰⁷ restrict the use of Customer Proprietary Network Information (CPNI), which is data processed by network carriers for the purpose of the transmission of a communication on a mobile device, including location data, and for the billing of such a communication.¹⁰⁸ The rules are designed to set limits and protect against the sharing and disclosure of consumer telephone data by carriers without the consumer's permission.¹⁰⁹

With regard to the processing of CPNI, the mobile user must have given prior consent (*opt-in*) in order for the carrier to transfer the data to a carrier's joint venture partners or independent contractors for the purpose of marketing communications-related services.¹¹⁰ However, a carrier may use CPNI to market products or services that the customer currently receives from that company without additional approval from the customer. Here, the carrier can choose between the *opt-in* and *opt-out* mechanism.¹¹¹ In order to receive consent from the mobile user, the carrier must request approval orally, in writing, or electronically. The request must include certain information about how the carrier will use the customer's CPNI. If CPNI is shared with joint venture partners or independent contractors, the carrier must ensure that the customer's CPNI is kept confidential. For example, if CPNI is disclosed to a marketing company, the carrier must review such a company before the disclosure of CPNI.¹¹²

Basically, U.S. mobile subscribers are more protected against unwanted commercial communications and have enhanced data protection rights than land-line subscribers because sending an electronic commercial solicitation to a wireless internet domain name (MSCM) or sending m-advertising using automated dialling equipment requires having the subscribers' express advance consent (i.e., analogous to EU rules of opt-in consent). Further, subscribers' personal data, to the extent that it is customer proprietary network information (CPNI), is protected from unauthorized use or disclosure unless the carrier obtains the subscribers' advance consent.

3.2.4. Security of personal information

Certain statutes have been adopted which apply to the security of personal data:

It is a federal crime to use pretexting to get access to individuals' personal information, such as *customer phone records information* (CPRI),¹¹³ under false pretences.¹¹⁴ The Telephone Records and Privacy Protection Act of 2007 (TRPPA)¹¹⁵ prohibits pretexting practices to buy, sell, or obtain CPRI.¹¹⁶ The 2007

¹⁰⁶ 47 U.S.C. § 151-710.

¹⁰⁷ See 2007 CPNI Order, para. 4.

¹⁰⁸ 47 U.S.C. § 222(h)(1)(A): CPNI is "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier." (The TCPA was amended in 1999 by the Wireless Public Safety Act of 1999 to include location data in the definition.)

¹⁰⁹ 47 U.S.C. § 222.

¹¹⁰ 2007 CPNI Order, at 37-50.

¹¹¹ Ibid., at App. B, Subpart U, 4.

¹¹² Federal Communications Commission (March 2008): *Protecting Your Telephone Calling Records*. Retrieved 08.05.2008 from <http://www.fcc.gov/cgb/consumerfacts/phoneaboutyou.html>.

¹¹³ 18 U.S.C. § 1039., at (h): CPRI is defined similar as CPNI: CPRI is information that "(A) relates to the quantity, technical configuration, type, destination, location, or amount of use of a service offered by a covered entity, subscribed to by any customer of that covered entity, and kept by or on behalf of that covered entity solely by virtue of the relationship between that covered entity and the customer; (B) is made available to a covered entity by a customer solely by virtue of the relationship between that covered entity and the customer; or (C) is contained in any bill, itemization, or account statement provided to a customer by or on behalf of a covered entity solely by virtue of the relationship between that covered entity and the customer"

¹¹⁴ For a detailed definition of *pretexting* please refer to Federal Communications Commission (February 2006): *Pretexting: Your Personal Information Revealed*. Retrieved 18.04.2008 from <http://www.ftc.gov/bcp/online/pubs/credit/pretext.shtm>.

¹¹⁵ 18 U.S.C. § 1039.

CPNI Order supplements the TRPPQ by requiring carriers to install security protection that will avoid the use of pretexting to obtain subscribers' CPNI.¹¹⁷

Moreover, the Electronic Communications Privacy Act of 1986 (ECPA)¹¹⁸ prohibits both the interception of the *contents* of electronic communication and the access to the *contents* of stored electronic communications.¹¹⁹ The provisions of the ECPA apply to all types of messages sent to mobile devices, unless the interception or unauthorized access is covered by exceptions or defences. It should be noticed that the ECPA is not a data protection law like the 2007 CPNI Order, because it only protects the contents of electronic communications from unlawful interception or access but not consumer privacy with respect to personal data. From this follows, using personal data such as phone numbers in order to send m-advertising messages would not be protected by the ECPA.¹²⁰

3.2.5. Consumer protection and self-regulation

As mentioned several times before, the U.S. approach is characterized as a market approach that focuses on fair information practices and privacy policies. Several mechanisms of industry self-regulation are tools to adopt fair information practices with respect to personal data of mobile device users. Such practices involve voluntary actions by companies to protect customers' personal data and to protect customers' from unsolicited commercial electronic communications. Third-party enforcement programs, such as *trust marks* or *privacy seals*, certify that a company's privacy policy meet certain information privacy standards such as FTC fair information practice principles of notice, choice, access, and security.¹²¹ Other programs to ensure fair information practices are adopted by industry associations in forms of *codes of conducts* that members must agree to follow¹²² or software programmes such as the Platform for Privacy Preferences (P3P).¹²³

4. Discussion

It is not possible to make a neat and clean comparison between EU and U.S. of fair information practices. However, there are some great differences between the two approaches and Daniel Solove aptly sums it: *"U.S. law has arisen haphazardly, in reactive fashion. The U.S. system is more fractured than other countries, so it's harder to pass broad, all-encompassing legislation. There are so many industries with well-paid lobbyists ready to pounce, the minute you propose anything of any breadth you are inundated with whiny companies that come in and shout 'Not me. Not me.' ... It's easier to do something pretty narrow and go after the 'now' problem and limit the amount of companies that are angry at you."*¹²⁴

It must also be taken into account that the above examination of the EU legal framework is more a guideline for EU nations, because each Member State has its own national law and agency that interprets that law. There are certain variations from country to country.

This section points out some great differences of the two approaches but also highlights the greatest weaknesses of them. Finally, some proposals for better regulation of m-advertising are made.

¹¹⁶ Ibid., at (a)-(c).

¹¹⁷ King (2008), p. 285.

¹¹⁸ 18 U.S.C. § 2510-2522, § 3117, and §§ 3121-3127.

¹¹⁹ Ibid., § 2511.

¹²⁰ See King (2008), pp. 285-90 for a detailed description of unlawful interception of and unauthorized access to mobile communications including court decisions which have narrowed down the ECPA's privacy protection.

¹²¹ Federal Trade Commission (June 2007): *Fair Information Practice Principles*. Retrieved 08.05.2008 from <http://www.ftc.gov/reports/privacy3/fairinfo.shtm>.

¹²² King (2008), p. 304, at footnote 325.

¹²³ See Cleff (2007), pp. 266-67. By means of this program Web site owners are able to answer a series of questions regarding their privacy policies and post their answers in a machine-readable code on their site. A P3P compatible browser compares the answers with its users' pre-set preferences and warns them of any practices that concern them. See also W3C (November 2007): *Platform for Privacy Preferences (P3P) Project: Enabling smarter Privacy Tools for the Web*. Retrieved 08.05.2008 from <http://www.w3.org/P3P/>.

¹²⁴ Sullivan (2006), quoting George Washington University Professor Daniel Solove.

4.1. Differences between the regulatory approaches applying to m-advertising

4.1.1. The value of information practices and the role of the government protecting it

While the EU and the U.S. share many values, the legal approaches in terms of protecting personal information differ most sharply, especially in competition with other goals, and on the influence of the government in protecting personal data. The EU legal framework is based on the principle that data protection should be treated as a fundamental right, on par with the freedom of expression and thoughts. In the U.S., in turn, a constitutional system prevails which highly values freedom of expression and of the press and the freedom from government intrusion into private affairs. Consequently, less value is placed on data protection and the government's limited power of regulating the private sector creates obstacles to the creation comprehensive legislations with respect to the protection of personal data.

The EU Data Protection Directive requires persons who wish to collect, process, use, store, and transfer personal data to register with their national data protection supervisory authority. Viewing the government as a guarantor of their rights, European citizens accept and often appreciate the government's intensive involvement in their daily lives. Conversely, in the United States, the government does not play an active role in guaranteeing citizens' rights. American society is traditionally sceptical of government, making it hard for the government to become involved in daily life to protect citizens' rights. Jane E. Kirtley explains: *"Privacy advocates urge the adoption of the European model for data protection in the name of protecting individual civil liberties. But in so doing, they ignore, or repudiate, an important aspect of the American democratic tradition: distrust of powerful central government. [...] when it comes to privacy, Americans generally do not assume that the government necessarily has citizens' best interests at heart. [...] The European paradigm assumes a much higher comfort level with a far more authoritarian government."*¹²⁵

While EU laws mandate a comprehensive data protection scheme enforced by national data protection commissioners, U.S. data protection is piecemeal. Where regulation exists in the U.S., there are differences between the treatment of public and private sectors, and industries. The differences of the two systems can be highlighted even better if one considers the contents of legislation. Above all European legislations empower consumers to remain control of their own information, based in particular on their prior consent to processing and on the right to access their personal data. Notification to the consumer and the national supervisory authority of the collection, use, and processing of personal data is required at several stages. In contrast, there are no federal provisions for a *"right to informational privacy"* in B2C transactions in the U.S. There are no omnibus rules with respect to the collection, use, and sharing of personal data that transcend all business sectors. Basically, a complex web of regulations exists that apply to m-advertising practices. The U.S. approach is characterized as a market approach to data protection that has created a focus on fair information practices and privacy policies.

4.2. Main differences between the legal frameworks applying to m-advertising

As observed in the previous section, the U.S. has no governmental agency with overall responsibility for the regulation of fair information practices. Though, EU Member States have adopted different supervisory models (e.g. a registration model in the U.K. and a licensing model in Sweden) there is a shared characteristics to have a centralized data protection supervisory authority of some sort.

As a general rule, the EU protects all personal data that lead to the identification of an individual and laws address all the instances of data collection, use, and sharing throughout the Union. In the U.S. only the use of CPNI data is protected by law. CPNI does, however, not include information such as customers' names, addresses and phone number or information derived from their use of information services. Also, the CPNI rules do not apply to carriers that conduct m-advertising related to their own communication services. Moreover, the collection, use, disclosure to third parties of mobile device numbers is not prohibited by any federal law and businesses may even create (computerized) databases of such numbers.

¹²⁵ Cate (1999), p. 226, quoting Jane E. Kirtley, former Executive Director of the Reporters Committee for Freedom of the Press.

There are also no requirements in U.S. law that consumers are allowed to inspect their own records and make corrections to them. The right to access one's own records and challenge their accuracy is given utmost importance in EU law, and this right extends across all sectors and across almost all data types. Secondary use of data is also treated differently in the EU and in the U.S. With very few exceptions, uses of personal data beyond the original purpose are prohibited in Europe if the consumer objects to the secondary usage. Federal U.S. law regulating CPNI do not generally require that consumers who have given consent for the use of such data must be told of secondary uses of data for another purpose.

Compared to the EU the U.S. has not implemented a uniform opt-in approach for the sending of m-advertising messages to consumers. Depending on what type of message is sent the opt-in (for MSCM) or the opt-out (for messages without a wireless Internet domain name) mechanism applies. Since advertisers may legitimately use consumers' mobile phone numbers to send conventional text messages (SMS), there is no absolute ban on sending unsolicited m-advertising. This is based on the assumption that the advertiser does not violate all other requirements stated in the FTC rules and TCPA as described in section 3.

The analysis above is only focusing on U.S. federal laws including rules applying to m-advertising. If a business, however, voluntarily adopts a privacy policy, it must keep its promises in order to avoid liability under the FTC rules. From this follows, there is a binding form of self-regulation in the U.S.

4.3. Weaknesses in the regulatory frameworks

4.3.1. European Union

The EU approach is characterized by highly specific legislations that protect personal data of consumers. However, the legal framework for processing data generated by different types of technologies for the purpose of personalized, location-based m-advertising is very complex. With three Directives that partially overlap, including a multitude of complicated definitions which can be interpreted in different ways, and the margin of implementation left to the Member States it is an enormous task to determine which legal provisions apply when advertisers process different types of data. Basically, there is no equal protection of personal data guaranteed within the different Member States.¹²⁶ Even though EU Member States must establish a supervisory data protection authority, different models exist.¹²⁷ Whereas the U.K. has embraced a registration model, providing a government agency with largely *reactive* power,¹²⁸ Sweden has adopted a licensing model, providing a federal bureau with *proactive* power.¹²⁹ As a result of the different models there are inconsistencies of enforcement of data protection rules among the Member States. There are consequently no harmonised guidelines for consumers on the conditions under which these agencies will enforce their rights.

Unclear definitions lead to open question especially with respect to the consent that must in certain cases be obtained for the processing of personal data: who exactly should give consent to whom, and how? What is an existing relationship and what is considered to be a similar product or service? How can a marketer know when an existing relationship ceases or when it exists? In addition, EU Directives often differentiate between B2C and B2B communications. However, the convergence of different technologies is changing these markets and brings the two closer while blurring the clear line between consumer and business activities.

The EU legal framework applying to m-advertising is characterized by extensive information requirements. Limitations in the user-interface of mobile devices create obstacles to comply with the requirements in an appropriate manner. Often different Directives with different requirements apply to same transaction, i.e. to m-advertising the E-Commerce Directive as well as the Distance Selling Directive applies. Advertisers may

¹²⁶ WP11 (2007), p. 12.

¹²⁷ Smith (2001), pp. 10-11.

¹²⁸ The registration model each database containing personal data to be registered by a separate governmental institution, which has the authority to *deregister* a data controller based on a complaint and investigation.

¹²⁹ The licensing model requires each database containing personal data to be licensed by a separate governmental institution, which stipulates the conditions for the collection, storage, use, etc. of personal data. This model requires prior approval by the institution for any processing of data.

face problems in fulfilling the requirements correctly while consumers may find it difficult to understand the different layers of information. Another problem is the amount of information which must be provided to the consumer. There is a risk of an information overload and the consumers may not be able to take in and process all the information before making any decision. Some obligations could be harmonized, for example, by standardization and presentation of information. This would also improve the manner in which information is communicated.

Moreover, there often exist a delay between the introduction of new technologies and business models and the implementation of legislations to protect personal data of the consumer. The dynamics of the information age lead to a generalized application information and communication technologies that tend to collect personal data beyond necessity, thereby creating a risk to consumers' privacy. EU Directives limit this risk, but the gap between the law and practice in the digital world expands.

4.3.2. United States

In the U.S., there is a tension between data protection and the freedom to disclose, disseminate, and receive information, which is protected by the First Amendment of the U.S. Constitution. The U.S. approach is based on the belief that the market will develop its own fair information practices without government intervention or legislation, and if it fails, then government regulation may be appropriate.¹³⁰ However, the economic incentive for businesses to protect personal data is quite weak and most serious proposals for self-regulation among market participants are dependent on government enforcement if the data collectors fail to regulate them effectively. If there are no commonly agreed standards or legal requirements in the first place, privacy policies may be avoided or changed at will. The latter procedure may, however, be challenged as an unfair or deceptive practice.

Moreover, the U.S. legal approach is not based on a technology-neutral principle. Different provisions apply to different forms of mobile communications (MSCM versus text messages) and competing advertisers offering basically same services find themselves under different regulatory regimes. Two federal agencies are in charge of the federal framework applying to m-advertising: The FTC adopts general regulations on spamming and the FCC adds to this regulation rules for spamming using wireless internet domain names. Consequently, advertiser sending MSCM must comply with both sources of regulation. However, there is not a single agency which is in charge of consumer complaints with respect to m-advertising. Moreover, the FCC is operating different kind of *Bureaus* such as the wireline, wireless, and media bureaus. It is said that the FCC should combine these bureaus into a new "*broadband bureau*" in order to better focus on functions within these converging sectors.¹³¹

Since mobile device users generally do not have privacy rights with respect to the use and disclosure of mobile device numbers, there is a risk that advertiser will ignore MSCM rules regarding the opt-in requirements when they are, for example, located outside the U.S. As mentioned before there exist no absolute ban on the sending of m-advertising and advertisers may circumvent CAN Spam, FTC, and TCPA rules quite easily. As long as businesses do not adopt a privacy policy, do not send m-advertising via MSCM, and do not use automated dialling equipment the sending of conventional text messages (i.e. phone-to-phone SMS or messages sent from a computer in form of a text message) is not prohibited, provided that such messages are not unfair or deceptive and include the labelling and other requirements stated in the FTC rules.

The drawback of a self-regulation approach is that there exist a whole flood of incentives and programs which differ considerably from each other. Since there are no commonly agreed-upon standards or legal requirements on key issues concerning data protection, each industry association, trustmark or code of conduct may proclaim different policies. Consumers are faced with different privacy policies and may lose the overview. It has been shown that consumers often fail to read or understand privacy policies and some

¹³⁰ Blumenfeld (1998), pp. 364-65, (making reference to the Clinton Administration's decision on a framework for Global Electronic Commerce, see Clinton and Gore (1997, July 1): Framework for Global Electronic Commerce. Retrieved 15.04.2008 from <http://isis.ku.dk/kurser/blob.aspx?feltid=196532>).

¹³¹ May (2008).

companies take advantage of it.¹³² Since businesses are not legally required to adopt privacy policies many may choose not to do so, making it difficult for the FTC to prosecute them for deceptive practices in terms of data protection. Also, since there are no universal rules about key principles which must be adopted when implementing a privacy policy, many companies may fail to address important data protection principles.¹³³ Harmonized standards are needed to guarantee adequate consumer protection and transparency. Moreover, without a strong commitment to ensuring adherence to policies, self-regulation will fail to ensure fair information practices. Many industry associations have the ability to enforce member companies' adherence. A self-regulatory approach is only meaningful if industry generated policies offer meaningful relief in instances of abuse.

5. Final remarks

Fair information practice is a central issue in m-advertising. This article has outlined two approaches which address this issue: the comprehensive legislative approach of the EU and the more industry-self-regulated market approach of the U.S. The concept of self-regulation is a very attractive one for businesses, especially because the legislative process is often slow to react to changing technologies and markets. Consumer trust is important for long-term marketing relationships and such trust can be achieved when companies adopt fair information practices and inform consumers about how their personal data will be treated. Consequently, the market may produce greater protection of personal data if companies adopt adequate privacy policies to attract and retain customers. However, legal conditions are necessary to create incentives for individuals and institutions to participate in a self-regulatory approach seriously because the desire to make profits seems to be overriding many company's guarantees as to their use of personal data.¹³⁴

Mobile devices are extremely personal items and consequently information gained from them can often be credited to a single user. Therefore, certain standards are needed to ensure fair information practices, such as purpose of the collection, use, and processing of personal data, a choice and access mechanism, and data retention requirements. Especially when it comes to secondary use of personal data, a market based approach may not be effective. Data that are retained become very vulnerable once they change ownership and a different company's privacy practices may apply. Therefore, legislation is needed to demand, at a minimum, that advertisers publish a privacy policy including the above mentioned principles. In other words, it is important to structure markets to guarantee that data protection is ensured and that non-compliance leads to legally enforceable remedies such as statutory damages.

Laws and regulations play a significant role in the development of m-advertising by providing guidance to advertisers and other involved parties about what they may do and not do. The legal framework specifying how consumers authorize access to their personal data must be clear, consistent, and technology-neutral. In an environment with convergence and interchangeable technologies, technological neutrality seeks to prevent that law and regulation quickly become outdated and enables to create a dynamic framework that can evolve with changing market conditions. Also, such an approach will lead to more consumer trust as it leads to more transparency. However, a technology-neutral approach is not a straightforward solution as it also poses challenges for the requirements and consumer protection rules. Such an approach will include wide, functional definitions which may be interpreted in different ways and it might be argued that such definitions will quickly lead to overregulation.¹³⁵ Moreover, there may still be contexts for m-advertising which include elements that may not allow services to be regulated equally.

Another approach, which has not been discussed earlier in this article, is the development of technical solutions that can contribute to fair information practices. Technology can intervene in two ways: on the one

¹³² O'Connor (2005), pp. 355-56.

¹³³ Haynes (2007), pp. 610-11.

¹³⁴ Nehf (2007), pp. 3-4: *The FTC placed its faith in market incentives to curb unfair privacy practices, but there may be little incentive for online businesses to adopt and adhere to strong privacy policies. It is the appearance of privacy that seems to matter most.*

¹³⁵ Haar (2007), p. 24. This could, for example, be the case for unregulated markets as technology neutrality would automatically lead to an extension or imposition of regulation even though such markets were fully competitive.

hand, they can be used to track personal data of consumers; on the other hand, they could also serve to protect data retention. The latter can be done in two ways, by either preventing the collection of identifying data before it accumulates, or technology can be used to anonymise data after collection has taken place.

The weaknesses of the EU and U.S. approaches have been pointed out and it can be concluded that a variety of strategies including legislation defining an overall set of standards, a structured market and privacy-enhancing technologies may serve as the best solution to contribute to fair information practices.

Evelyn Beatrix Cleff (*EBCL@asb.dk*) *College of Business - Oregon State University (USA)*
Affiliate Faculty: Aarhus School of Business, Aarhus University (Denmark)

References

1. Legislation

1.1. European Union

Charter of Fundamental Rights of the European Union, OJ C 364, 18.12.2000.

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 ('Data Protection Directive'), OJ L 281, 23.11.95.

Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts ('Distance Selling Directive').

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ('Directive on privacy and electronic communications'), OJ L 201, 31.7.2002.

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), OJ L 149, 11.6.2005.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC ('Data Retention Directive'), OJ L 105, 13.04.2006.

European Union: Consolidated Versions of the Treaty on European Union and of the Treaty establishing the European Community, OJ C 321E, 29.12.2006.

European Convention for the Protection of Human Rights and Fundamental Freedoms, November 4, 1950, 213 U.N.T.S. 221.

Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation. COM(2007) 698 final, 13.11.2007.

1.2. United States

1.2.1. Federal Laws

The United States Constitution adopted on September 17, 1787.

Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act), 15 U.S.C. §§ 7701-7713 and 18 U.S.C. § 1037.

Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-2522, § 3117, and §§ 3121-3127.

Federal Trade Commission Act (FTC Act), 15 U.S.C. §§ 41-58 (2007).

The Telecommunication Act of 1996, 47 U.S.C. § 151-710.

Telephone Consumer Protection Act of 1991 (TCPA), 47 U.S.C. § 227.

Telephone Records and Privacy Protection Act of 2007 (TRPPA), 18 U.S.C. § 1039.

Wireless Public Safety Act of 1999, 47 U.S.C. § 609.

1.2.2. Administrative Laws

Final Rule, Definitions and Implementation under the CAN-SPAM Act of 2003, 16 C.F.R. § 316 (2003).

Rules and Regulations implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Rules and Regulations implementing the Telephone Consumer Protection Act of 1991 (FCC's Mobile Spam Regulations), 47 C.F.R. Part 64.3100, FR 55765-01.

Rules and Regulations implementing the Telecommunication Consumer Protection Act of 1991, *Report and Order* [hereinafter 2003 TCPA Order], 18 F.C.C.R. 14014 (2003).

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.R. 6927 (2007) [hereinafter 2007 CPNI Order].

2. Case Law

2.1. European Union

ECJ, C-288/89, *Collectieve Antennevoorziening Gouda and others v. Commissariaat voor de Media* [1991], ECR I-4007 (judgment of 25 July 1991).

ECJ, C-352/85, *Bond van Adverteerders and others v. The Netherlands State* [1988], ECR 2085 (judgment of 26 April 1988).

ECJ, C-390/99, *Canal Satélite Digital v. Administración General del Estado* [2002], ECR I-6087 (judgment of 22 January 2002).

ECJ, C-377/98, *the Netherlands v. European Parliament and Council of the European Union* [2001], ECR I-07079 (judgment of 9 October 2001).

European Court of Human Rights, *Handyside v. United Kingdom* (Appl. No. 5493/72), judgment of 7 December 1976, Ser. A, No. 24.

European Court of Human Rights, *Sunday Times v. the United Kingdom* (Appl. No. 6538/74), judgment of 26 April 1979, Ser. A, No. 30.

European Court of Human Rights, *von Hannover v. Germany* (Appl. No. 59320/00), judgement of 24 June 2004.

2.2. United States

Central Hudson Gas & Electric Corp. v. Public Service Commission, 447 U.S. 557 (1980).

Cliffdale Association, Inc., 103 F.T.C. 110 (1984).

International Harvester Company, 104 F.T.C. 949 (1984).

Board of Trustees of State Univ. of N.Y. v. Fox, 492 U.S. 469 (1989).

R.A.V. v. City of St. Paul, 505 U.S. 377 (1992).
U.S. v. Edge Broadcasting, 509 U.S. 418 (1993).
U.S. v. Hambrick, 55 F. Supp. 2d 504 (1999).
FTC v. Gateway Learning Corp., File No. 042-3047 (2003).
FTC v. Toysmart, File No. 00-11341-RGS (filed July 10, 2000).

3. Books, Journal Articles, and Reports

Article 29 Working Party (2007): *Opinion on the concept of personal data*. WP 136 EN (20.06.2007).
Article 29 Working Party (2005): *Opinion on the use of location data with a view to providing value added services*. WP 115 EN (25.11.2005).
Barnes, Morey Elizabeth (2006): Falling Short of the Mark: The United States Response to the European Union's Data Privacy Directive. *Northwestern Journal of International Law & Business*, 27(1), 171-97.
Blanchette, Jean-François and Deborah G. Johnson (2002): Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness. *Information Society*, 18(1), 33-45.
Blumenfeld, Elizabeth de Grazia (1998): Privacy Please: Will the Internet Industry Act to Protect Consumer Privacy before the Government. *Business Lawyer*, 54(1), 349 - 80.
Boedecker, Karl A., Fred W. Morgan and Linda Berns Wright (1995): The Evolution of First Amendment Protection for Commercial Speech. *Journal of Marketing*, 59(1), 38-47.
Cate, Fred H. (1999): The Changing Face of Privacy Protection in the European Union and the United States. *Indiana Law Review*, 33, 173-232.
Cleff, Evelyn Beatrix (2007): Implementing the legal criteria of meaningful consent in the concept of mobile advertising. *Computer Law & Security Report*, 23(3), 262-69.
Clinton, William J. and Albert Gore (1997): Framework for Global Electronic Commerce [Electronic Version]. Retrieved 24.04.2008 from <http://isis.ku.dk/kurser/blob.aspx?feltid=196532>.
Cohen, Julie E. (2000): Examined Lives: Informational Privacy and the Subject as Object. *Stanford Law Review*, 52, 1373-437.
Commentary of the Charter of Fundamental Rights of the European Union, prepared by the EU Network of Independent Experts on Fundamental Rights, 20 June 2006 [Electronic Version]. Retrieved 25.04.2008 from http://ec.europa.eu/justice_home/doc_centre/rights/charter/docs/network_commentary_final%20_180706.pdf.
Gratton, Eloïse (2002): M-Commerce: The Notion of Consumer Consent in Receiving Location Based Advertising. *Canadian Journal of Law and Technology*, 1(3), 59-77.
Haynes, Allyson W. (2007): Online Privacy Policies: Contracting Away Control Over Personal Information? *Penn State Law Review*, 111(3), 587-624.
Hildner, Laura (2006): Defusing the Threat of RFID: Protecting Consumer Privacy through Technology-Specific Legislation at the State Level. *Harvard Civil Rights Civil Liberties Law Review*, 41(1), 133-76.
Haar, Ilse M. van der (2007): Technological Neutrality; What Does it Entail? [Electronic Version]. *TILEC Discussion Paper*. Retrieved 01.05.2008 from <http://ssrn.com/abstract=985260>.
Joinson, Adam N. and Carina B. Paine (2007): Self-disclosure, Privacy and the Internet (chapter 16). In Joinson, A., K. McKenna, T. Postmes and U. Reips (Eds.), *The Oxford Handbook of Internet Psychology* (pp. 237-52). New York: Oxford University Press.
Kang, Jerry (1998): Information Privacy in Cyberspace Transactions. *Stanford Law Review*, 50, 1193-294.
King, Nancy J. (2008): Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices. *Federal Communications Law Journal*, 60(2), 229-324.

May, Randolph J. (2008, February 25): Perspective: At FCC, change must be the mantra [Electronic Version]. *cnet NEWS.com*. Retrieved from http://business2-cnet.com.com/At-FCC%2C-change-must-be-the-mantra/2010-1033_3-6231729.html?tag=item.

Nehf, Jim P. (2007): Shopping for Privacy Online: Consumer Decision Making Strategies and the Emerging Market for Information Privacy. *Journal of Consumer Affairs*, 41.

Nielsen, Ruth and Christina D. Tvarnø (2005): *Retskilder & Retsteorier*: Jurist- og Økonomforbundets Forlag.

O'Connor, Peter (2005): Comparative Analysis of International Approaches to the Protection of Online Privacy (chapter 14). In Krishnamurthy, S. (Ed.), *Contemporary Research in E-Marketing* (Vol. 2, pp. 347 - 64). Hershey PA, USA: Idea Group Publishing.

OECD: *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (from 23 September 1980) [Electronic Version]. Retrieved 14.03.2008 from http://www.oecd.org/document/18/0,3343,es_2649_34255_1815186_1_1_1_1,00.html.

Rozen, Jeffrey (2000): *The Unwanted Gaz: The Destruction of Privacy in America*. New York: Knopf Publishing Group.

Schwartz, Paul M. and Joel R. Reidenberg (1996): *Data privacy law: a study of United States data protection*. Charlottesville, VA: Michie Law Publisher.

Shaffer, Gregory (1999): The Power of EU Collective Action: The Impact of EU Data Privacy Regulation on US Business Practice. *European Law Journal*, 5(4), 419.

Smith, H. Jeff (2001): Information Privacy and Marketing: What the U.S. should and shouldn't learn from Europe. *California Management Review*, 43(2), 8-33.

Solove, Daniel J., Marc Rotenberg and Paul M. Schwartz (2005): *Information Privacy Law*. New York: Aspen Publishers.

Sullivan, Bob (2006): EU citizens well protected against corporate intrusion, but red tape is thick [Electronic Version]. *Privacy Lost: EU, U.S. laws differ greatly*. Retrieved 30.04.2008 from <http://www.msnbc.msn.com/id/15157222/>.

Tsai, Robert L. (2004): Speech and Strife. *Law and Contemporary Problems*, 67(83), 83-104.

Westin, Alan (1967): *Privacy and Freedom*. New York: Atheneum.

Whitman, James Q. (2004): The Two Western Cultures of Privacy: Dignity versus Liberty. *Yale Law Journal*, 113(6), 1151-221.

WP11 (2007): *D11.5: The legal framework for location-based services in Europe* (Report): FIDIS Consortium.

4. Websites

European Commission (September 2007): EU and the World - External Trade: *Bilateral Trade Relations*. Retrieved 23.04.2008 from http://ec.europa.eu/trade/issues/bilateral/countries/usa/index_en.htm.

European Commission (27.04.2007): *Facts and Figures on the European Union and the United States*. Retrieved 23.04.2008 from <http://www.eurunion.org/profile/facts.htm>.

European Commission (March 2007): Mobile and Wireless Communications, Relevant Policies: *Mobile & Wireless Communications: Lowering Costs, Stimulating Growth*. Retrieved 28.03.2008 from http://ec.europa.eu/information_society/industry/comms/mobile/pol/index_en.htm.

Federal Communications Commission (March 2008): *Protecting Your Telephone Calling Records*. Retrieved 08.05.2008 from <http://www.fcc.gov/cgb/consumerfacts/phoneaboutyou.html>.

Federal Communications Commission (29.02.2008): *About the WTB*. Retrieved 15.04.2008 from <http://wireless.fcc.gov/index.htm?job=about>.

Federal Communications Commission (01.10.2007): *Consumer Policy Issues, Can Spam, Unwanted Commercial Electronic Mail*. Retrieved 16.04.08 from <http://www.fcc.gov/cgb/policy/DomainNameDownload.html>.

Federal Communications Commission (01.05.2007): FCC Consumer Facts: *CAN-SPAM: Unwanted Text Messages and E-Mail on Wireless Phones and other Mobile Devices* Retrieved 16.04.08 from <http://www.fcc.gov/cgb/consumerfacts/canspam.html>.

Federal Communications Commission (February 2006): *Pretexting: Your Personal Information Revealed*. Retrieved 18.04.2008 from <http://www.ftc.gov/bcp/online/pubs/credit/pretext.shtm>.

Federal Trade Commission: Privacy Initiatives: *Introduction*. Retrieved 16.04.08 from <http://www.ftc.gov/privacy/>.

Federal Trade Commission: SPAM: *for Consumers Page*. Retrieved 16.04.08 from <http://www.ftc.gov/bcp/online/edcams/spam/consumer.htm>.

Federal Trade Commission (29.03.2008): *About the Federal Trade Commission*. Retrieved 15.04.2008 from <http://ftc.gov/ftc/about.shtm>.

Federal Trade Commission (June 2007): *Fair Information Practice Principles*. Retrieved 08.05.2008 from <http://www.ftc.gov/reports/privacy3/fairinfo.shtm>.

SCADPlus (31.08.2007): Information Society: *Protection of personal data*. Retrieved 09.04.2008 from <http://europa.eu/scadplus/leg/en/lvb/l14012.htm>.

W3C (November 2007): *Platform for Privacy Preferences (P3P) Project: Enabling smarter Privacy Tools for the Web*. Retrieved 08.05.2008 from <http://www.w3.org/P3P/>.