


3-2008

# Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices

Nancy J. King  
*Oregon State University*

Follow this and additional works at: <http://www.repository.law.indiana.edu/fclj>

 Part of the [Administrative Law Commons](#), [Communications Law Commons](#), [Consumer Protection Law Commons](#), and the [Legislation Commons](#)

## Recommended Citation

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*: Vol. 60: Iss. 2, Article 4.  
Available at: <http://www.repository.law.indiana.edu/fclj/vol60/iss2/4>

This Article is brought to you for free and open access by the Law School Journals at Digital Repository @ Maurer Law. It has been accepted for inclusion in Federal Communications Law Journal by an authorized administrator of Digital Repository @ Maurer Law. For more information, please contact [wattn@indiana.edu](mailto:wattn@indiana.edu).

# Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices

Nancy J. King\*

- I. INTRODUCTION ..... 231
- II. MOBILE COMMERCE AND MOBILE ADVERTISING..... 234
- III. M-ADVERTISING RAISES PRIVACY CONCERNS FOR CONSUMERS ..... 239
- IV. PRIVACY REGULATION AND MOBILE ADVERTISING..... 247
- V. FEDERAL PRIVACY REGULATION AND M-ADVERTISING ..... 250
  - A. *Breach of Privacy Policies as Unfair Trade Practices*.... 252
  - B. *Spamming as an Unfair Trade Practice* ..... 256
    - 1. “Opt-out” Consent is the Minimum Required to Send Unsolicited Advertising Accessed on Mobile Phones..... 260
    - 2. “Opt-in” is Required to send M-Ads Directly to Mobile Phones Using MSCMs..... 261

---

\* Associate Professor, Oregon State University, College of Business, 200 Bexell Hall, Corvallis, Oregon 97331-2603, 541-737-3323, kingn@bus.oregonstate.edu. J.D., M.S.T., Gonzaga University. The author expresses gratitude to the Fulbright Program, the J. William Fulbright Foreign Scholarship Board, and the Commission for Educational Exchange between the United States of America, Belgium and Luxembourg European Union Program for the award of a 2007-2008 fellowship to support her research on privacy issues related to global regulation of mobile communications technologies. This Article provides the U.S. law foundation for a U.S./European Union comparative law study of privacy issues related to mobile communications technologies.

C.	<i>Telemarketing as Unfair Trade Practices</i> .....	265
1.	The Telemarketing Sales Rule .....	265
2.	The Telephone Consumer Protection Act .....	267
D.	<i>Mobile Carriers' Obligations to Protect Phone Subscribers' Personal Data</i> .....	271
1.	Customer Proprietary Network Information. ....	276
2.	Subscriber List Information and Access to Mobile Phone Numbers .....	280
3.	Federal Preemption Limits State Law Regulation of Telecommunications Carriers That Aim to Enhance Telephone Subscribers' Personal Data Protection .....	282
4.	Legislative and Administrative Proposals Aim to Enhance Consumer Privacy Protections for Telephone Records and Mobile Phone Numbers....	283
E.	<i>Obtaining Subscribers' Phone Records by "Pretexting" Is a Federal Crime</i> .....	284
F.	<i>Federal Statutes Protect Mobile Phone Users' Communications from Unlawful Interception or Unauthorized Access</i> .....	285
VI.	STATE PRIVACY LAWS AND M-ADVERTISING .....	290
A.	<i>State Consumer Privacy Laws Address Unfair and Deceptive M-Advertising Practices</i> .....	291
B.	<i>Common Law Privacy Torts May Apply to M- Advertising Practices</i> .....	292
C.	<i>Common Law Contract Principles May Limit or Facilitate M-Advertising Practices—Focus on Mobile Services Agreements</i> .....	297
VII.	IS FEDERAL PRIVACY REGULATION ADEQUATE TO PROTECT CONSUMER PRIVACY IN M-ADVERTISING?.....	301
A.	<i>Consumer Privacy and the Market Approach to Data Protection</i> .....	302
B.	<i>Privacy Policies Should Provide Notice and Disclose Company Privacy Practices</i> .....	304
C.	<i>Industry Models for Privacy Policies for M-Advertising</i> . 307	
D.	<i>Fair Information Practices for M-Advertising Must Include Obtaining Appropriate Consumer Consent</i> .....	310
1.	Using Form Agreements to Obtain Consumer Consent.....	312
2.	The Use of Privacy Enhancing Technologies as an Alternative to Privacy Policies.....	314

- E. *Why the Market Approach to Data Privacy Does Not Currently Ensure Appropriate Consumer Consent for M-Advertising* ..... 315
  - 1. Voice Calls Made to Mobile Phones ..... 315
  - 2. Electronic Messages Sent to Mobile Phones ..... 316
  - 3. Ads Displayed on Web Sites Accessed with Mobile Phones ..... 318
  - 4. Ads Generated by Adware or Spyware Loaded on Cell Phone Handsets ..... 319
- F. *Proposal for Regulatory Reform to Ensure Appropriate Consumer Notice and Consent for M-Advertising* ..... 320
  - 1. The Need to Protect the Confidentiality of Cell Phone Numbers ..... 320
  - 2. The Need for Meaningful Short Privacy Notices for Mobile Advertising ..... 321
  - 3. The Need for Additional Protections Related to Consumer Location Data ..... 322
- VIII. CONCLUSION ..... 324

I. INTRODUCTION

Mobile commerce is gradually emerging as a new commercial environment in the U.S., facilitated by the increasing numbers of consumers who have mobile phones and other portable wireless electronic communications devices.<sup>1</sup> No longer simply a mobile telephone, mobile phones offer new communications and information services.<sup>2</sup> Mobile

---

1. It is estimated that over two billion people worldwide have cell phones. Roger O. Crockett, *Will That Be Cash, Credit, or Cell?*, BUSINESSWEEK, June 27, 2005, at 42 (arguing that mobile commerce seems poised to make a lasting comeback). See also Teresa F. Lindeman, *XLNT Deals 4 U!: Companies Turn to 'Mobile' Commerce*, PITTSBURGH POST-GAZETTE, Oct. 22, 2006, available at <http://www.post-gazette.com/pg/06295/731760-28.stm#> (reporting on recent cell phone marketing efforts by businesses in the U.S. including the fact that marketers' use of mobile commerce in the United States has lagged behind that of other countries like Europe, Japan, and Korea); Eric Pfanner, *Mobile Phones Are New Frontier in Advertising*, INT'L HERALD TRIBUNE, Mar. 11, 2007, (on file with author) (reporting that approximately one billion mobile phones will be sold in the world in 2007).

2. Mobile phones come equipped with data, text, and video streaming functions, making them much more than simple devices for making phone calls. International Telecommunications Union, *The Internet of Things 25-26* (Geneva 2005) (reporting on technologies that will create a "ubiquitous network society," including RFID and smart computing, and the important role of mobile phones as a portal to that network society) [hereinafter *Seventh ITU Internet Report*], available at <http://www.itu.int/internetofthings/>. "With the development of mobile internet and mobile commerce service, users can buy theatre tickets, make hotel reservations, and access bank accounts through their mobile

commerce will enable consumers to use their mobile phones to conveniently purchase goods and services (like parking passes or theater tickets) and to receive timely information content (like directions and maps).<sup>3</sup> Mobile commerce is also generating new advertising opportunities for suppliers of new and existing products and services directed at consumers through their mobile phones.<sup>4</sup> Consumers may welcome mobile advertising or view it as an annoyance. In either case, this Article argues that consumers and advertisers should be concerned about protecting consumers' privacy and personal data in this new environment.

Two key privacy concerns for U.S. consumers arising from mobile advertising practices are: 1) the collection, use, and disclosure of consumers' personally identifying information that accompanies mobile advertising; and 2) the generation of unsolicited mobile advertising.

---

phones." *Id.* at 26. "Mobile phones are now a significant source of personal information, such as phone numbers, calendar, photos, messages, passwords and so on." *Id.* In the future, mobile phones will provide "an important portal to new enhanced services," and the players in the telecommunications industry will shift their focus from providing voice communications to data transmission. *Id.* at 69.

3. The term mobile phone is used in this Article to refer to a communications device that in the U.S. may commonly be referred to as a cell phone or a wireless phone. Deborah F. Buckman, Annotation, *Construction and Application of "Personal Wireless Service Facility" Provision of Federal Communications Act, 47 U.S.C.A. § 332(c)(7)(C)(ii)*, 2006 A.L.R. FED. 2D 1, § 2 (2006). A mobile phone:

is actually a radio containing a low power transmitter. When a wireless telephone is turned on, it searches for a base station within range. . . . The base station relays identifying information to a local mobile telephone switching office which confirms that the telephone is assigned to a valid customer and then assigns a frequency on which the user may communicate.

*Id.*

4. Generally, mobile commerce (m-commerce) describes business transactions conducted using wireless devices that allow consumers to make purchases from any location with service for their wireless devices. The technological development that facilitates m-commerce is known as wireless application protocol ("WAP"). Alfred Villoch III, *Europe's Mobile Opportunity: Can the European Union Legislate Consumer Trust and Compete in the E-Commerce Market with the United States?*, 20 PENN. ST. INT'L L. REV. 439, 446 (2002). WAP allows users of mobile phones to interact with information and services immediately by accessing "the Internet through the phone's small screen. . . . [Consumers] can make purchases and reservations, or request directions by simply using the phones' buttons. . . and engage in e-commerce without having to use a desktop" or even a laptop computer with wireless capability. *Id.* at 447. Essentially, with WAP, consumers' mobile phones act as mini Web browsers. The mobile phones' mini browsers display "specially formatted web pages from the Internet. If the contacted web site does not offer this special web page format, then the handset [of the mobile phone] is unable to display this site." *Id.* See also James C. White, *People, Not Places: A Policy Framework for Analyzing Location Privacy Issues*, Masters Memo Prepared for the Electronic Privacy Information Center (Spring 2003), available at <http://www.epic.org/privacy/location/jwhitelocationprivacy.pdf>. M-commerce businesses may utilize use location information about consumers to create content "whose value comes from knowledge of where a user physically is, such as traffic or weather information." *Id.* at ii.

Advertisers, mobile telecommunications carriers (mobile carriers), mobile phone manufacturers (handset manufacturers), and other third parties may all be involved in generating or delivering m-advertisements. For example, advertisers may direct their messages to consumers' mobile phones by calling mobile phone numbers to talk directly with consumers or generating voice, text, instant, or multimedia messages (e.g., video clips) to be delivered directly to or accessed by consumers on their mobile phones. Advertisements may also be displayed on mobile phones when consumers access Web sites using their Internet-access-equipped mobile phones. Adware programs loaded directly on consumers' phones by handset manufacturers or downloaded to cell phones from the Internet are yet another way to deliver mobile advertising. When the available methods of delivering mobile advertising are considered in conjunction with technological advances enabling advertisers to target advertising to consumers based on the geographic location of their mobile phones at a particular time (personalized location and time-specific advertising), the enormous potential of the mobile advertising market is apparent. Not so obvious are the consumer privacy implications and the very real possibility that consumers will view mobile advertising as privacy intrusive.<sup>5</sup>

The primary goal of this Article is to assess the adequacy of existing U.S. laws designed to protect consumers' privacy and personal data with respect to advertising directed at or accessed by consumers through their mobile phones and other wireless communications devices.<sup>6</sup> The Article argues that consumers are entitled to fair information practices associated with mobile advertising that should include at least the right to receive meaningful notice and to give their informed consent to the collection, use, and disclosure of their personal information. It also argues that consumers have the right to choose whether to receive mobile advertisements. The Article offers insights and recommendations from a federal regulation and/or industry self-regulation perspective to ensure that mobile advertising directed at consumers will be accompanied by these two components of fair information practices. It is essential to find consumer privacy solutions for

---

5. See *Recent Development, Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 307-11 (2004) [hereinafter *Recent Development in HARV. J.L. & TECH.*] (explaining how cell phones work to provide location information about the cell phone user in the context of potential governmental abuses of cell phone data). This Article will address nongovernmental uses and abuses of cell phone data including using location information for commercial purposes such as advertising.

6. Although there are a variety of wireless communications devices that consumers may use to obtain the communications services provided by mobile phones (e.g., BlackBerry handheld devices), the term mobile phones is used in this Article to collectively refer to portable wireless communications devices that consumers may use to participate in mobile commerce.

mobile advertising in order to build consumer trust that will enable the newly emerging mobile advertising industry to grow and flourish.

## II. MOBILE COMMERCE AND MOBILE ADVERTISING

Mobile phones may well be the next big consumer marketing opportunity.<sup>7</sup> M-advertising is a form of mobile commerce (also referred to as m-commerce or mobile e-commerce).<sup>8</sup> In m-commerce, wireless devices such as mobile phones, wireless-enabled handheld computers, vehicle-mounted technologies, and personal message paging devices are used to connect to mobile services.<sup>9</sup> M-commerce applications include m-advertising that is directed at or accessed on consumers' mobile phones, such as advertising sent in text messages to consumers.<sup>10</sup> As used in this Article, mobile advertising includes direct marketing as well as other forms of advertising accessed on mobile phones.<sup>11</sup> Mobile advertising has

---

7. Pfanner, *supra* note 1.

8. Peter Tarasewich et al., *Issues in Mobile E-commerce*, 8 COMM'NS OF THE ASS'N FOR INFO. SYS. 41, 42 (2002) (defining m-commerce as "all activities related to a (potential) commercial transaction conducted through communications networks that interface with wireless (or mobile) devices."). Mobile commerce encompasses a wide range of interactive business processes that occur before, during, and after actual sales transactions. *Id.* See also Sridhar Balasubraman et al., *Exploring the Implications of M-Commerce for Markets and Marketing*, 30 J. ACAD. MARKETING SCI. 348, 349-50 (2002) (providing a five component conceptualization of m-commerce that is separate from the underlying technologies related to mobile communications devices).

9. Tarasewich et al., *supra* note 8, at 42.

10. *Id.* at 51. Mobile advertising refers to ads sent to and displayed on mobile communications devices including mobile phones and other handheld wireless communications devices. Jaana Tähtinen & Jari Salo, *Special Features of Mobile Advertising and their Utilization*, Proceedings of the 33rd EMAC conference at 2 (2004), available at <http://www.taloustieteet oulu.fi/arvoa-luovat/Julkaisut/Tahtinen%20and%20Salo%202004%20Special%20features%20of%20mobile%20advertising%20and%20their%20utilization.pdf>. Research on emerging business models for mobile advertising has three essential elements: the advertising service (which includes the chosen technology used to deliver the m-ads to the consumers' mobile devices), the roles of the actors in providing the advertising service, and the value-creating exchanges between the actors. Hanna Komulainen et al., *Business Models in the Emerging Context of Mobile Advertising*, FRONTIERS OF E-BUSINESS RESEARCH at 590, 592 (2004) available at [http://www.ebrc.info/kuvat/590-605\\_04.pdf](http://www.ebrc.info/kuvat/590-605_04.pdf). As yet, successful business models for generating revenues from mobile advertising are still being developed. The business actors that are involved in creating value through mobile advertising include: 1) an application provider (software vendor who develops the software system needed for mobile advertising); 2) advertiser (creates the content in terms of mobile ads for a mobile advertising system); 3) infrastructure provider (provides the network infrastructure needed to run the services); 4) mobile network operator (rents the network from the infrastructure provider in order to provide access to the wireless network and enable the sending of m-ads); 5) mobile service provider (offers the mobile advertising service system to content providers); and 6) end-user (consumer who receives the mobile ads). *Id.* at 592.

11. The global "Mobile Marketing Association (MMA) defines 'mobile marketing' as 'the use of wireless media as an integrated content delivery and direct response vehicle

advantages over print or broadcast advertising because it allows marketers to send location- and time-specific, personalized advertisements directly to consumers.<sup>12</sup>

A brief example of m-advertising shows how it will provide new avenues for advertisers to reach consumers with their messages:

A person working in an office takes a break for lunch. Walking out of his office to buy some lunch, he receives a text message on his mobile phone advertising a lunch special at a nearby restaurant. The text message includes a discount coupon for the restaurant's lunch special. Several technologies enable the advertiser to sense that a cell phone is located near its restaurant and to direct a text message to this particular phone.<sup>13</sup> In this scenario, the consumer may benefit from having his mobile phone handy. If he is interested in visiting the restaurant, he may use it to call the restaurant for reservations and directions or to phone ahead to place an order and save time. He may also appreciate the discount coupon, which he can use by displaying it on his mobile phone. On the other hand, he may find this advertising practice quite annoying, perhaps akin to retailer stalking.

Although m-commerce applications are gradually being introduced to U.S. consumers, the above scenario is not yet commonplace in the U.S. Examples include the *Wall Street Journal Online's* offers to subscribers to receive stock price and volume trading alerts on their mobile phones.<sup>14</sup> Subscribers with Web-enabled mobile devices may also receive "the latest

---

within a cross-media marketing communications program." Laura Marriott, *Mobile Marketing: Back to the Basics*, THE CLICKZ NETWORK, Nov. 16, 2006, <http://www.clickz.com/showPage.html?page=3623954>. For a discussion of the distinction between advertising, including online advertising, and direct marketing, see SIMMONS & SIMMONS, E-COMMERCE LAW, DOING BUSINESS ONLINE 119-36 Palladian Law Publishing Ltd., Isle of Wight (2001) (providing an overview of the regulation of online advertising and direct marketing in the United Kingdom). Generally, online advertising uses nonbroadcast media, and the content is available for viewing on a one-to-many basis; however, transmission of that content does not happen simultaneously but rather occurs when the Web site is accessed by each individual user. Direct marketing is a business practice that involves communicating promotions of businesses' products and services directly to individuals, whether by telephone, fax, email, or other methods. Direct marketing generally involves processing personal data about consumers. *Id.* at 119-21.

12. Jari Salo & Janna Tähtinen, *Retailer Use of Permission-Based Mobile Advertising*, in Irvine Clarke III & Teresa B. Flatherty, *Advances in Electronic Marketing* Chapter VIII (2005); Working Party 29, Working Party 29 Opinion on the Use of Location Data with a View to Providing Value Added Services (Nov. 2005) available at [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2005/wp115\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf) (includes discussion of uses of location data and mobile telephony).

13. These technologies include triangulation, Global Positioning System ("GPS"), and radio frequency identification devices ("RFID"). GPS and RFID technologies are explained in more depth later in this Article.

14. What's News on Your Phone, DOWJONES ONLINE, <http://alerts.dowjones.com/Alerts> (last visited Feb. 25, 2008).



Wall Street Journal financial and business stories, technology news, opinion and stock quotes on [their] BlackBerry®, Treo® or other mobile devices.”<sup>15</sup> Another example is provided by the Foot Locker retail chain. Foot Locker collected several hundred thousand cell phone numbers from consumers in a program that spanned over three years. It then used them to send promotions by text messages to customers who had agreed to receive the promotions.<sup>16</sup> Moreover, Sprint, a telecommunications company, introduced a service in 2006 that allows fans of the National Football League (“NFL”) to pay a fee to get information about NFL games on their cell phones. In 2007, the company offered an improved version for free to most of its customers.<sup>17</sup> Recently, Amazon.com began allowing customers to shop using Web-enabled cell phones, and Yahoo! began testing a program that allows advertisers to pay for sponsored search results through its Mobile Web service.<sup>18</sup> Also, Verizon Wireless recently announced that it would soon be placing banner ads on its customers’ cell phone displays, known as “on deck.”<sup>19</sup> In December 2007, Microsoft also announced that it was bringing ads to mobile devices.<sup>20</sup>

Currently, marketers in Europe, Japan, and Korea use m-commerce applications such as m-advertising at higher rates than marketers in the U.S.<sup>21</sup> Explanations for this difference in m-commerce adoption rates include the availability of standardization in mobile communications technology in locations outside the U.S. and the increased likelihood that cell phones in Europe will have Web browsers as compared to cell phones in the U.S.<sup>22</sup> Another factor discouraging m-advertising applications in the

---

15. *Get Mobile*, THE WALL STREET JOURNAL ONLINE, <http://mobile.wsj.com/> (last visited Feb. 25, 2008) (currently these services are only available through corporate enterprises).

16. Lindeman, *supra* note 1 (reporting that about one of every 5,000 customers who signed up for the Foot Locker program later opted-out of the program).

17. *Id.*

18. *Id.*

19. ELECTRONIC PRIVACY INFORMATION CENTER, 2006 PRIVACY YEAR IN REVIEW, (Jan. 4, 2007), [http://www.epic.org/alert/EPIC\\_Alert\\_yir2006.html](http://www.epic.org/alert/EPIC_Alert_yir2006.html) (reporting that even a cell phone in an off position sends a signal that enables location tracking of the cell phone user).

20. Elinor Mills, *Microsoft Bringing Ads to Mobile Devices*, CNETNEWS.COM (Dec. 10, 2007) (reporting that beginning December 10, 2007, visitors to the MSN portal will be able to see mini banner ads optimized for their browser type and screen size).

21. Lindeman, *supra* note 1. *See also* Pfanner, *supra* note 1 (reporting that an online publishers’ survey showed that thirty-seven percent of Europeans are receptive to the idea of watching ads in exchange for free mobile content while only eighteen percent of respondents in the U.S. were receptive to this idea).

22. *Id.*; *see also* Villoch III, *supra* note 4, at 443-46. Villoch explains that the three primary reasons for Europe’s mobile advantage over the United States. First, deregulation of European national telecommunications markets allows mobile service providers to enjoy legal and technical uniformity among the nations and to provide consumers with competitive service pricing. *Id.* at 444-45. Second, the establishment of a single cross-border

U.S. is that text messaging often costs the user more than regular cell phone calls. So U.S. consumers may resist receiving text messages from marketers due to the cost differential.<sup>23</sup> Despite the slow adoption rate for m-advertising in the U.S., a consulting firm estimates the global market for mobile advertising may reach \$9.6 billion by 2010.<sup>24</sup>

The availability of mobile phone-specific Web site addresses is also expected to encourage m-commerce and associated m-advertising as mobile phone users gain access to Web sites that have been optimized for mobile phone access.<sup>25</sup> Wireless and Internet companies around the globe, including companies in the U.S., recently agreed on a set of development guidelines for the design of Web sites that are easy to navigate using mobile devices.<sup>26</sup>

A key factor related to consumer acceptance of m-commerce and m-advertising is likely to be the relationship between consumer privacy and consumer trust.<sup>27</sup> As discussed in the next section of this Article, there are

---

wireless transmission standard in the European Union, compared to the development in the U.S. of multiple cellular standards (quoting Walt Mossbert, *Technology: Walt Does Wireless*, WALL ST.J., Sept. 29, 2000, at W1: “[the U.S. has an] incompatible hodgepodge of towers, services and phones.”). *Id.* at 445. Third, European countries’ constitutions do not contain free speech requirements that are as strict as those found in the U.S. Constitution, enabling the European Union to legislate uniform guidelines on data protection and consumer privacy. *Id.* at 445-46.

23. Lindeman, *supra* note 1. *See also* Villoch, *supra* note 4, at 443-46.

24. *See* Electronic Privacy Information Center, *supra* note 19.

25. The Internet Corporation for Assigned Names and Numbers (“ICANN”) approved “.mobi” as a top level domain (“TLD”) name that will be restricted to mobile devices and Web sites providing services for them. ICANN, ICANN Publishes Proposed Agreement on .MOBI (June 3, 2005), <http://www.icann.org/announcements/announcement-03jun05.htm>. The global registry for the .mobi TLD names is mobile Top Level Domain Ltd. (dotMobi). dotMobi, About Us, <http://pc.mtld.mobilenet/aboutus.html> (last visited Feb. 25, 2008). Appointed by ICANN as the registry for .mobi TLDs, dotMobi is backed by leading mobile operators, network device manufacturers, and Internet content providers. *Id.* *See also*, *Mobile Web Shake-up Gets Started*, BBC NEWS (Sept. 25, 2006) available at <http://news.bbc.co.uk/2/hi/technology/5379170.stm?ls>. BBC NEWS reports the start of open registration for mobile phone-specific Web site addresses (Mobile Top Level Domain (“MTLD”)) in the U.K. Sites ending with “.mobi” must meet agreed standards for optimizing Web sites for use by mobile phones, which should ensure users a consistent experience. Currently “[o]nly one in 10 mobile owners use their phones to surf the net due to concerns over cost, speed and poor content,” but this new top level domain name registration is expected to encourage the growth of m-commerce. *Id.*

26. *See* Mobiledia, Industry Leaders Agree on Rules for Mobile Web Sites (June 27, 2006), <http://www.mobiledia.com/news/48070.html?rfp=dta>; WORLD WIDE WEB CONSORTIUM, MOBILE WEB BEST PRACTICES 1.0: BASIC GUIDELINES, (Jo Rabin & Charles McCathieNeville, eds. Nov. 2, 2006), <http://www.w3.org/TR/mobile-bp/>. Among other things, the guidelines advise developers against using big graphics or pop-up ads that could clutter phone screens and using cookies. *Id.*

27. *See* Villoch, *supra* note 4, at 442 (explaining how timely legislation is an important factor in gaining consumer trust, and discussing the European Union’s efforts to require

important privacy concerns for U.S. consumers related to m-advertising that cell phone users in other countries may not face. For example, consumers in many other developed countries, including those in Canada and the twenty-seven member states of the European Union, already have broad-based privacy regulations that protect their privacy and personal data.<sup>28</sup> In contrast, no analogous broad-based consumer privacy regulations exist in the U.S.<sup>29</sup> Although telecommunications carriers are heavily regulated in the U.S., and mobile phone subscribers in the U.S. have some enhanced privacy protections over landline customers, the direct marketing industry in the U.S. is not heavily regulated. As a result, direct marketers are generally free to use consumers' personally identifying information to generate advertising and direct marketing to mobile subscribers, subject to regulations that limit the generation of unsolicited advertising messages.<sup>30</sup>

---

Member States to implement current data protection legislation in their national laws in order to advance e-commerce in the EU).

28. Gail Lasprogata et al., *Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada*, 2004 STAN. TECH. L. REV. 4, ¶¶ 9-15 (2004), [http://str.stanford.edu/STLR/Articles/04\\_STLR\\_4](http://str.stanford.edu/STLR/Articles/04_STLR_4). Even where broad-based privacy regulation exists to protect consumer privacy, the emergence of new technologies, like RFID-enabled mobile phones, challenge regulators to apply their privacy laws in this new context. See Press Release, European Commission, Commission Proposes a European Policy Strategy for Smart Radio Tags (Mar. 15, 2007), [http://ec.europa.eu/information\\_society/newsroom/cf/itemdetail.cfm?item\\_id=3247](http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=3247) (announcing that the European Commission proposes to address the privacy concerns of citizens to boost consumer confidence and Europe's position in a market experiencing sixty percent growth globally; the report came one year after the European Commission announced an extensive Europe-wide consultation on radio frequency identification (RFID) tags).

29. DANIEL J. SOLOVE & MARK ROTENBERG, *INFORMATION PRIVACY LAW* 9-38 (2006) (providing an overview of information privacy protections under U.S. law); Laura Hildner, *Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level*, 41 HARV. C. R. -C.L. LAW REV. 133, 138 (2006) (arguing that advocates of baseline privacy legislation in the U.S. are unrealistic because they fail to recognize the political barriers to such legislation and their proposals are inconsistent with the historical approach of regulating privacy in the U.S.). See also Christopher S. Rugaber, *High-Tech Firms to Push for Data Privacy Law*, MSNBC, Dec. 8, 2006, available at <http://www.msnbc.msn.com/id/16115003/orig/1/displaymore/1098/> (“[H]igh-tech companies are preparing to push for data-privacy legislation [in 2007] to replace what they consider an outdated patchwork of state and federal laws that are inconsistent and burdensome.”).

30. Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 142-43 (2006). Ludington summarizes the profound lack of consumer privacy that exists in the U.S. today with respect to the direct marketing industry:

[T]he direct marketing industry is free from government regulation of its data trading practices, with the exception of the Do-Not-Call list imposed by the Federal Communications Commission (FCC) in 2003. . . . [M]ost types of personal information – including names, birthdates, addresses, telephone numbers, clickstream data, travel details (flights, car rentals, hotels, train tickets) and transactional data (who bought what from whom, when, where, and how) – are

For this reason, consumer privacy and data protection concerns need to be analyzed in light of current laws and industry self-regulation to assess the adequacy of protections for U.S. consumers who will be the focus of m-advertising.

### III. M-ADVERTISING RAISES PRIVACY CONCERNS FOR CONSUMERS

Mobile advertising raises several significant consumer privacy concerns that are summarized in Exhibit A. First, m-advertising raises privacy concerns associated with mobile phones and other portable wireless communications devices because it often involves the collection, use, or disclosure of consumers' personal data.<sup>31</sup> Emerging business models for m-advertising often assume that the advertiser has access to a database that includes consumers' cell phone numbers and other personally identifying information ("PII").<sup>32</sup> Cell phone numbers, records of calls made and received, and billing information of cell phone subscribers are all forms of PII about cell phone subscribers that are potentially useful to m-advertisers. For example, a mobile telecommunications carrier may desire to use

---

unregulated, unless the data trader violates its own privacy policy, in which case the Federal Trade Commission (FTC) can hold the company accountable for unfair trade practices. Thus it is currently legal – in the sense that there is no penalty – for data traders to sell personal information without the consent of the subject, to deny individuals information about the quantity or categories of lists that contain their information, and to deny any requests to remove personal information from these lists. Even regulated data traders, such as banks and credit reporting agencies, are permitted to share personal information with their "affiliates" without permission from the affected individuals.

*Id.* (internal citations omitted). Direct marketing to mobile phones is also limited by federal spam laws. See discussion of Mobile Service Communications Messages (MSCMs), *infra* Section V.B.

31. Informational privacy is one concept of privacy that addresses an individual's rights to control his or her personal information. See SOLOVE & ROTENBERG, *supra* note 29, at 49 (arguing there are six different categories that conceptualize privacy including informational privacy, but that they are not independent of each other; "[f]or example, control over personal information can be seen as a subset of limited access to the self, which in turn bears significant similarities to the right to be let alone"). Under Canadian law, the right to informational privacy has been described as "the right of the individual to determine for himself when, how, and to what extent he will release personal information about himself." Lasprogata et al., *supra* note 28, at ¶11. Under European law this right is defined in terms of "personal data." See Data Privacy Directive, Council Directive 95/46/EC, 1995 O.J. (L 281) [hereinafter Privacy Directive].

32. See Komulainen et al., *supra* note 10, at 596-601 (examining business models that utilize two technologies of sending mobile ads to consumers: the first technology involves sending mobile ads to consumers as multimedia messages that the consumer receives in the same way as tradition Short Messaging Service ("SMS") or text messages; in the second technology, consumers are sent a service indicator message that includes a description of a mobile ad and an URL address, and consumers can then decide whether to browse the actual mobile ad). Implicit in these business models is the use of consumer databases containing at least the wireless phone numbers of consumers. *Id.* at 600.

customers' mobile phone numbers to generate additional revenues by conveying ads to its cell phone subscribers.<sup>33</sup> These ads may be designed to sell additional communications services offered by the mobile telecommunications carrier or its joint venture partners. Alternatively, a third party advertiser may advertise its products and services to cell phone subscribers. One way to do this would be for the advertiser to establish a relationship with a mobile carrier in which the carrier would provide access to its subscribers for the purpose of delivering advertising messages. Or, the third party advertiser could collect consumers' cell phone numbers from some other source, perhaps a commercial data trader.<sup>34</sup>

A fourth model is newly emerging that may radically change how consumers receive cell phone service and the new model may significantly impact the challenges of privacy regulation to ensure the adequacy of consumer notice and consent for mobile advertising. This new model is currently exemplified by Google's announcement of its cell phone strategy—the "Android platform."<sup>35</sup> Google's cell phone strategy goes well

---

33. Matt Richtel, *Verizon to Allow Ads On Its Mobile Phones*, N. Y. TIMES, Dec. 26, 2006, at C5. According to Richtel:

Verizon Wireless, among the nation's most widely advertised brands, is poised to become the advertising medium itself. Beginning [in 2007], Verizon Wireless will allow placement of banner advertisements on news, weather, sports and other Internet sites that users visit and display on their mobile phones, company executives said....

Verizon officials said their initial foray would be a cautious one – they will limit where ads can appear, and exclude certain kinds of video clips – and thus may invite greater demand to place ads than they can accommodate.

"We know we can make significant dollars in mobile Web advertising in 2007," said John Harrobin, vice president of marketing and digital media for Verizon Wireless. "That said ... we want to take it carefully and methodically, and enable the right experience." More generally, he added, "Mobile advertising is going to take off in 2007."

*Id.* This article reported that in October 2006, Sprint became the first major carrier to allow advertisements to appear with content that is listed on its menus (known as "on-deck advertising" in the cell phone industry; in contrast, advertising that is "off-deck" refers to advertising placed on content sites that wireless customers may access over the Internet). *Id.* See also Electronic Privacy Information Center, *supra* note 19, at 5.

34. See Ludington, *supra* note 30, at 142. Ludington describes a "data trader" as:

[A]ny private entity that collects, stores, processes, sells, rents, or disseminates personal information, including, but not limited to, a data broker. Data traders may include businesses such as direct marketers, retail establishments, on-line businesses (including Internet Service Providers), service industries (such as travel agents) and data brokers – entities whose sole business is to collect, analyze, and trade personal information.

*Id.*

35. Marguerite Reardon and Elinor Mills, *Google unveils cell phone software and alliance*, CNET NEWS.COM (Nov. 7, 2007) (commenting that the Android platform "consists of an operating system, middleware, a user-friendly interface and applications"). According to Google's CEO Eric Schmidt: "Consumers should expect the first phones based on Android to be available in the second half of 2008." *Id.*

beyond prior indications that Google was developing a new cell phone (the Gphone) that would be supported by advertising revenue.<sup>36</sup> Significantly, Google recently announced that it is forming an alliance of companies that provide wireless communications services, including leading mobile carriers, chip makers, and mobile handset manufacturers.<sup>37</sup> This consortium is working together to develop an open platform cell phone application that will include new mobile phone software to serve as an operating system for mobile phones.<sup>38</sup> But, unlike current mobile operating systems on the market that have been developed by companies like Apple, Microsoft, Nokia, Palm, and Research in Motion, the Android platform will not be tied to specific devices.<sup>39</sup> Instead, the new mobile operating system will work with a broad variety of devices from handset makers. Also, because the Google project proposes an open mobile operating platform, it will facilitate the development of mobile service applications by third party developers.<sup>40</sup>

Consistent with the Google business model, advertising revenues may enable consumers to receive their mobile phones, telecommunication services, and other mobile services (like Internet access, map services, etc.) for free or at reduced cost.<sup>41</sup> This is in contrast to the current model, which requires consumers to pay carriers for their mobile phone service and to pay carriers or other service providers for mobile service applications. Of course, it is likely that “free” or reduced cost to consumers may come with a price tag that requires consumers to give up personal information and

---

36. Elinor Mills, *More Google Phone rumors*, CNET NEWS.COM (Oct. 29, 2007). *See also*, Marguerite Reardon, *Google pitches Gphones to Verizon*, CNET NEWS.COM (Oct. 30, 2007); Elinor Mills, *In search of the Google phone*, CNET NEWS.COM (Oct. 24, 2007) (speculating that the Gphone would be advertising supported based on filing of a patent application by Google for advertising-supported telephony); Amol Sharma, *Can a Google Phone Connect With Carriers?*, THE WALL ST. J., Oct. 30, 2007, at B1 (commenting that “Google-powered phones are expected to wrap together several Google applications – among them, its search engine, Google Maps, YouTube and Gmail email – that have already made their way onto mobile devices.” *But see*, Charles Cooper, *Parsing the Google announcement that wasn’t*, CNET NEWS.COM (Nov. 9, 2007) (commenting on continuing speculation over whether Google will bid on an upcoming FCC auction for wireless spectrum or buy wireless spectrum, which would allow Google to build a network to accommodate a Google phone, or instead, partner with existing network carriers that will run its mobile applications hardware).

37. Marguerite Reardon & Elinor Mills, *Google unveils cell phone software and alliance*, CNET NEWS.COM (Nov. 7, 2007).

38. *Id.*

39. *Id.*

40. *Id.*

41. Sharma, *supra* note 36, at B1 (commenting “[i]f Google isn’t careful, sensitive user information could end up in the wrong hands, leading to spamming, stalking other invasions of privacy.”).

privacy.<sup>42</sup> The privacy price tag may include consumer acquiescence to the receipt of mobile advertising and for the use and disclosure of their personally identifying information and even location data to facilitate m-advertising.

### Exhibit A

#### Overview of Personal Data and Privacy Issues Related to Mobile Advertising—The Federal Regulatory Framework

Contexts of Personal Data Collection, Use, etc.	Examples	Current Federal Privacy Regulation
<b>Collection and Use of Consumers' Mobile Phone Numbers and Consumer Purchasing History</b>	Consumer's mobile (cell) phone number becomes available to advertisers and is used to generate unsolicited or solicited mobile advertising calls and text messages. Consumer's PII, purchasing history, etc. collected by one business and sold to third parties for advertising and other purposes.	No generally applicable federal data protection regulation protects consumers' PII from m-advertising uses. Breach of promises in m-advertisers' privacy policies may be enforced by the FTC as unfair or deceptive trade practices. "Opt-in" consent required for telemarketing solicitations made directly to cell phones using wireless Internet domain names on the FCC's official list (e.g., email, text, multi-media, audio ads); but collection/access/disclosure of mobile phone numbers is not regulated—also mobile phone numbers are not CPNI under rules covering mobile carriers. Prohibitions on using auto-dialing telephone equipment to deliver mobile ads without prior express consent of called party may operate to limit m-advertising uses of cell phone numbers.
<b>Geographic Location Data of Consumer Cell Phones</b>	Mobile user's geographic location is detected by a mobile carrier or third party and used to generate location and time specific advertising.	Location data is a form of CPNI so mobile carriers' use/disclosure of this data for marketing purposes is regulated. Location data collected by noncarriers (e.g., advertisers) is not regulated and probably is not "contents" of communications, so not protected by ECPA.
<b>Data Aggregation/Consumer Dossiers</b>	Commercial data banks collect consumer's PII and offer it for sale to advertisers including cell phone numbers, telephone call detail, etc.	New federal pretexting statute makes it a crime to use deception to collect CPNI from a carrier and also restricts sale of consumers' CPNI unlawfully obtained by pretexting. New FCC regulations on CPNI require "opt-in" subscriber consent for carriers' disclosure of CPNI to joint-venture partners for marketing purposes, which may reduce flow of telephone record data to data aggregators.
<b>Unsolicited Advertising that Unreasonably Intrudes on Consumers in Private or Public</b>	Mobile spam including text and instant messages sent to consumer's mobile phone. Consumer often must pay for text and	CAN-SPAM requires "opt-in" consent to send commercial advertising directly to a mobile device, if to do so utilizes a wireless Internet domain name on the FCC's official list, unless the electronic message is sent under the transactional or relationship exception.

42. *Id.*

<b>Space</b>	instant messages whether solicited or not and whether read or not.	CAN-SPAM requires only “opt-out” consent to send commercial advertising to consumers when it is not sent directly to a mobile device, even if it is accessed using consumer’s mobile phone. Only opt-out consent is required to send phone-to-phone SMS (text messages) that do not utilize a wireless Internet domain name.
<b>Interception of Private Cell Phone Communications</b>	Mobile user’s credit card numbers and passwords intercepted by third parties monitoring m-commerce transactions	ECPA makes it a civil and a criminal offense for anyone to unlawfully intercept or access in storage the contents of a voice, wire, or electronic communication. See exceptions for providers of communications systems and consent.

Location privacy is a second concern raised for consumers by m-advertising. It is possible for mobile phone service providers and other third parties (even those consumers may not be aware of) to electronically track the geographic locations and Web surfing behaviors of mobile phone users.<sup>43</sup> The mobile phone user’s cell phone number and a unique Mobile Identification Number (“MIN”)<sup>44</sup> (assigned by the manufacturer to each mobile phone and unchangeable by the user) make it possible for mobile phone carriers using signal triangulation processes to track an individual cell phone user by tracking the location of his or her mobile phone.<sup>45</sup>

---

43. See Laurie Thomas Lee, *Can Police Track Your Wireless Calls? Call Location Information and Privacy Law*, 21 CARDOZO ARTS & ENT. L.J. 381 (2003) (commenting that call location information technology promises a wealth of benefits for users and may produce a dream for advertisers, including the development of mobile location services market worth billions but also raises privacy issues for Americans who may find their own cell phones have become location tracking devices for government use). See also MobileInfo.com, *The Mobile Computing Market: The Big Picture*, <http://www.mobileinfo.com/market.htm> (last visited Feb. 25, 2008); John Dunbar, *Cell Phones Lack Reliable Tracking for 911*, THE ASSOCIATED PRESS, Apr. 24, 2007, available at <http://www.msnbc.msn.com/id/18294965/>. FCC regulation requires companies that use network technology (triangulating among cell phone towers to determine the caller’s location) to locate callers in emergencies to come within 300 meters of the caller ninety-five percent of the time and requires companies that use handset technology (global positioning satellite (“GPS”) technology to locate callers) to come within 150 meters ninety-five percent of the time. A recent study by the Association of Public Safety Communications International (“APCO”) of mobile carriers’ ability to meet the FCC standards, which encompassed tests conducted in seven different communities across the U.S., showed that the companies were unable to meet these standards a significant portion of the time. *Id.*

44. See Recent Development in HARV. J.L. & TECH, *supra* note 5, at 309. The FCC set a deadline after which cell service providers must supply location information so that emergency callers from cell phones can be located within 150 meters; however, the specific type of location technology that cell service providers use to meet this requirement was not legislated. *Id.* at 308. So, for example, there is no law that requires cell phones sold in the U.S. to have GPS chips.

45. Signal triangulation is a process used to estimate a mobile phone’s location based on the relative positions of the different cellular receiving towers that carried signals from the user’s phone. Timothy Joseph Duva, Comment, *You Get What You Pay For ... and So*



Location-tracking technologies utilizing Global Positioning Service (“GPS”) technologies also enable mobile phone carriers to locate and track individual mobile phones.<sup>46</sup> Further, RFIDs<sup>47</sup> may soon be embedded in

---

*Does the Government: How Law Enforcement Can Use Your Personal Property to Track Your Movements*, 6 N.C. J. L. & TECH. 165, 169 (2004).

Each tower in a provider’s network is equipped with radio intercepts that receive signals from any active cell phone. When two or more of these towers receive signals from the same phone, the towers are able to compare the signals and locate the unit in one of two ways: Time Difference of Arrival (“TDOA”) or Angle of Arrival (“AOA”).

When a cell phone connects with a provider’s tower using a TDOA system, the tower measures the amount of time it takes for the signal to leave one location and reach the other. . . . These time measurements make it possible to estimate the distance between the tower and the phone. When more than one tower can do so, an algorithm allows the system to determine coordinates corresponding to the phone’s latitude and longitude.

Much like the TDOA system, angle-of-arrival technology [AOA] uses signals between the cell tower and wireless phone to determine location. Rather than measuring the time it takes for the signal to travel between the two positions, however, the tower records the angle at which the phone’s signal arrives at the station. When multiple towers receive signals, the system can compare the angles of arrival and thus triangulate the relative location of the cell phone. . . .

In urban areas, the number of towers and their sectioning into directional “faces” (north face, south face, etc.) gives providers access to quite accurate location information. While making a single phone call, your signal can move between different cell towers or faces on a single tower, creating a virtual map of your movements. In rural settings, the location information available to providers is significantly less accurate simply because fewer towers are available. In some areas, cell service is provided by a single tower covering several hundred square miles. Neither TDOA nor AOA techniques can triangulate locations in such circumstances.

Recent Development in HARV. J.L. & TECH., *supra* note 5, at 308-09. Signal triangulation does not yield location data as precise as that generated by GPS systems. Duva, *supra* note 45, at 169. One limitation of triangulation is that it does not work if the user’s mobile phone is turned off. Recent Development in HARV. J.L. & TECH., *supra* note 5, at 309.

46. Kristen E. Edmundson, Note, *Global Positioning System Implants: Must Consumer Privacy Be Lost in Order for People to Be Found?*, 38 IND. L. REV. 207, 209 (2005) (explaining what GPS is and how it works). Mobile phones equipped with GPS allow mobile communication networks to give the exact geographic position of mobile phones so equipped, and thereby permit tracking of people in possession of the GPS-equipped mobile phones. See Villoch, *supra* note 4, at 448-49. “[GPS] enables providers to pinpoint the position of a GPS-enabled cell phone anywhere on the globe.” Recent Development in HARV. J.L. & TECH., *supra* note 5, at 308. GPS works by measuring the time it takes for a signal to travel the distance between satellites and a cell phone’s GPS chip. When the GPS chip receives four synchronized signals from GPS satellites, it can calculate a three-dimensional location that is accurate to within twenty meters. However, GPS does have certain disadvantages. Because the system depends on receiving information from satellites, it does not perform well when trees, buildings, or other barriers obstruct access. *Id.* The information produced by GPS technologies could be used by advertisers to provide location-specific advertising messages, to provide traffic information and guidance to drivers, and to aid with 911 emergency services. See Villoch, *supra* note 4, at 448-49.

47. Laura Hildner provides an excellent description of RFID systems. RFID systems have three components: a tag, a reader, and a database. First, a silicon chip and antenna combination (hereinafter RFID tag) that can be attached to or incorporated into consumer

mobile phones, enabling communication between advertisers and consumers with RFID-equipped phones.<sup>48</sup> Though currently limited by short read-range, RFID-equipped mobile phones in combination with RFID readers that have been strategically placed by advertisers and databases that are connected to the Internet will facilitate location tracking of consumers. Once location data about consumers' mobile phones has been collected and stored in a database, it may be uploaded to the Internet for potential use by others. To the extent that mobile phone location tracking data becomes available to m-advertisers, it will be possible to target consumers on a location- and time-specific basis. Although the data will probably be useful

---

goods (including a mobile phone). The tag may include an electronic product code ("EPC"), but unlike the bar code currently imprinted on many consumer products, it may be encrypted with a unique code that makes individual products individually identifiable (particularized information). The RFID tag may be as small as a grain of sand and thus unnoticeable by consumers. The tag's antenna transmits the tag's particularized information. Second, RFID systems include a RFID reader (reader). Readers use radio waves to scan tags to obtain their data. Readers may be mobile or stationary and come in variable sizes and powers. A tag used for commercial purposes generally does not have a battery and operates at ultrahigh frequencies, such that readers can access them at a range between three and fifteen feet. RFID systems have an advantage over EPC systems because the RFID reader can read information from tags even if the tag is not in their line of sight and the reader can process multiple tags at the same time. Third, RFID systems include a database. The RFID database receives the information programmed onto tags that has been read by the reader. The RFID database can link information received from the tag to product information and potentially to information about the person who possesses the consumer item with the tag. Hildner, *supra* note 29, at 134-35. For a detailed overview of consumer applications of RFID technologies, see FEDERAL TRADE COMMISSION, RADIO FREQUENCY IDENTIFICATION: APPLICATIONS AND IMPLICATIONS FOR CONSUMERS (March 2005), available at <http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf> [hereinafter FTC RFID Workshop Report].

48. David Meyer, *Operators Want RFID in Phones*, ZDNET.CO.UK, Nov. 20, 2006, <http://news.zdnet.co.uk/communications/0,1000000085,39284785,00.htm> (reporting that the GSM Association ("GSMA"), representing operators that service more than eighty-two percent of the world's phone users, is pushing for a global standard on near field communications ("NFC")). Such a global standard would address short-range wireless technology that is based on having an RFID chip embedded in mobile phone handsets combined with NFC software. Wide-ranging applications for such technology include enabling mobile phones to serve as a key for the phone user's car that could open the car door and put the right music on the car stereo. An RFID-equipped phone with NFC software could also act as a payment device in stores or to download concert tickets that would then be recognized by an RFID reader at the concert venue. *Id.* See also John M. Eden, *When Big Brother Privatizes: Commercial Surveillance, The Privacy Act of 1974, and the Future of RFID*, 2005 DUKE L. & TECH. REV. 20, 20 (2005); Seventh ITU Internet Report, *supra* note 2, at 56 (reporting on the emerging trend of integrating RFID in mobile handsets and the prediction by ABI Research that of the estimated 830 million new mobile phones shipped in 2009, 30 percent will be NFC compliant); Beth Bachelder, *Nokia Uses RFID-Enabled Phones to Police Its Security Guards*, RFID JOURNAL, Dec. 18, 2006, <http://www.rfidjournal.com/article/articleview/2904/1/1/>, (reporting that mobile phones carried by security guards at the company are outfitted with RFID tags in the handset and an RFID reader in its outer shell, enabling the company to track its security guards as they patrol buildings, parking areas, and common grounds).

for advertising purposes only for a limited time period as consumers will also be mobile, consumers may view collection and use of location data by advertisers to be an annoying intrusion into their privacy that is akin to stalking.

A third privacy concern for consumers is that m-commerce creates a risk that consumers' personal data will increasingly be the focus of data aggregators.<sup>49</sup> Without adequate privacy regulation, advertisers, mobile carriers, and other third parties may combine consumers' personal data, the contents of their electronic communications, and geographic location information with other data about consumers that is already in electronic databases, thus creating larger consumer profiles with associated privacy implications.

A fourth privacy concern is the likelihood that unsolicited advertising will increasingly be received on consumers' mobile phones, thus intruding on consumers' personal space and time in both public and private spheres. M-ads may become as ubiquitous as unwanted spam in the email environment but are likely to be more bothersome given that consumers are likely to have their phones turned on and with them nearly all the time.

The privacy concerns associated with m-advertising are exacerbated when it is recognized that consumers' personal data gathered for legitimate business purposes may be used for wrongful or criminal purposes. Although m-advertising contexts will include advertisements and direct marketing communications designed to truthfully advertise products or services to consumers, there is also the possibility that consumers' personal information, electronic communications, and location data may be used for improper or even criminal purposes, such as committing identity theft, fraud, or electronic stalking. It is often said that privacy and security go hand-in-hand—to the extent that the mobile commerce environment lacks essential privacy protections for consumers, consumers may unwittingly expose their credit card numbers and passwords to those who would commit fraud or identity theft.<sup>50</sup>

---

49. See, e.g., Lars S. Smith, *RFID and Other Embedded Technologies: Who Owns the Data?*, 22 SANTA CLARA COMP. & HIGH TECH. L.J. 695, 695 (2006) (exploring the extent to which someone can own or control the information contained on RFID tags); Eden, *supra* note 49, at 23-24 (concluding extant privacy law is not adequate to protect consumers from potential abuses of new surveillance technologies like RFID).

50. See Villoch III, *supra* note 4, at 439-40 (providing a hypothetical example of bank fraud committed by gaining unauthorized access to a consumer's wireless banking transmissions made via Internet-enabled mobile phone). Recently the Mexican Association of Banks warned customers about a new type of fraud being committed through cellular phones that involves sending fraudulent calls that can destroy the phone's mechanism, duplicate phone numbers, capture codes, and create new ones. See *MX-ABM Warns of New Type of Fraud*, GLOBAL E-LAW ALERT, Baker & McKenzie and Contributing Firms, Dec. 11, 2006 (on file with author).

This Article now turns to examining the adequacy of U.S. laws that regulate m-advertising as well as efforts by m-advertisers and other industry representatives to protect consumers' privacy through industry self-regulation, company-specific fair information practices, and giving consumers technological solutions that they may choose to employ.

#### IV. PRIVACY REGULATION AND MOBILE ADVERTISING

Federal legislation provides minimal privacy of protections for consumers using mobile phones.<sup>51</sup> Exhibit A analyzes some of the contexts in which these privacy concerns may arise, including examples of anticipated ways that advertisers will collect and use the contents of consumers' mobile communications and/or their PII for m-advertising purposes and a summary of the applicable federal privacy laws, if any. State legislatures in each of the fifty states also have the power to adopt state statutes to protect the privacy and personal data of consumers.<sup>52</sup>

There are two primary federal administrative agencies that regulate business practices involving using, disclosing, or providing access to consumers' PII related to their mobile phones. First, the Federal Trade Commission ("FTC") is responsible for administering and enforcing laws

---

51. Federal legislation is supplemented by federal administrative regulations and by orders and decisions issued by administrative agencies. See LAWRENCE M. FRIEDMAN, *AMERICAN LAW IN THE 20TH CENTURY* 170-73 (2002) (explaining the development of administrative agencies, administrative law, and the role of Congress and the courts in limiting the power of administrative agencies). Final administrative regulations and administrative agency orders and decisions are legally binding on businesses operating in the U.S. For example, federal administrative regulations that have been drafted by administrative agencies, published for notice and comment, and then adopted by administrative agencies as final regulations are binding sources of law in the U.S. For this reason, administrative law is a source of regulation for the business practices of companies that provide mobile phone service to U.S. consumers and companies that target U.S. consumers with mobile phones for advertisements of products and services. Further, under the common law legal system in effect in the U.S., courts consider cases and issue opinions containing their decisions in the cases. Court opinions often contain judicial interpretations of legislation and administrative law, including whether an administrative order or decision is enforceable. These court opinions are binding legal precedents to be applied in subsequent cases involving similar disputes. *Id.*

52. Unless preempted by federal law, states may adopt state laws that protect consumer privacy, including adding privacy protections that exceed federal privacy laws. Daniel J. Solove & Chris J. Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 402. Solove and Hoofnagle comment that historically federal privacy laws have not preempted stronger state consumer privacy laws or administrative enforcement efforts. *Id.* They argue that most privacy legislation in the United States has been enacted at the state level and list examples of this type of state privacy legislation. *Id.* Further, they comment on the innovation by the states at the administrative enforcement level that has exceeded that of the federal administrative agencies, for example that it was the states, not the FTC, that first acted to create telemarketing Do Not Call lists. *Id.*

that address unfair or deceptive trade practices.<sup>53</sup> For example, if a business has a privacy policy that promises that customers' PII will not be disclosed to third parties, and that business discloses a customer's PII (such as her cell phone number or email address) to third-party advertisers without the customer's consent, this practice may be an unfair or deceptive trade practice that is within the FTC's enforcement powers.<sup>54</sup> However, a business that reveals customers' PII only violates federal law if doing so is contrary to the privacy promises the business has made to its customers, such as promises made in a privacy policy or a services contract between the customer and the business.<sup>55</sup> This is so because no federal law requires an advertiser or other private business (other than a mobile carrier) to adopt a privacy policy or to make promises to protect the consumers' privacy and personal data.<sup>56</sup> Generally, however, if a business adopts such a policy or makes privacy promises to consumers, it is an unfair or deceptive trade practice to break those promises.<sup>57</sup> The FTC also enforces specific federal statutes designed to regulate unfair and deceptive forms of spam and telemarketing and is responsible for maintaining the National Do Not Call Registry.<sup>58</sup>

The second federal agency responsible for regulating business uses of mobile phone users' personal data is the Federal Communications Commission ("FCC").<sup>59</sup> The FCC administers and enforces privacy statutes and regulations related to using, disclosing, and providing access to consumers' personal data by telecommunications carriers, including mobile carriers.<sup>60</sup> For example, if a mobile carrier releases certain types of personal

---

53. See Federal Trade Commission, About the Federal Trade Commission, <http://ftc.gov/ftc/about.shtml> (last visited Feb. 25, 2008).

54. 15 U.S.C. § 57a(a)(1)(b) (2007) (providing FTC enforcement authority that covers unfair or deceptive acts or practices that occur in or affect interstate commerce).

55. *Id.*

56. There are limited industry segments that have obligations to adopt privacy policies and protect consumers' personal data. See Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, 44 AM. BUS. L.J. 55, 74 (2007) (discussing the four major industry sectors where federal law regulates privacy policies including: "(1) children under the age of thirteen – covered by the Children's Online Privacy Protection Act of 1998 (COPPA), (2) financial institutions – covered by the Gramm-Leach-Bliley Act of 1999 (GLBA), (3) health care providers/institutions – covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and (4) federal government agencies, covered by the E-Government Act of 2002 (EGA).").

57. *Id.*

58. 15 U.S.C. § 6102 (2001) (empowering the FTC to prescribe rules prohibiting deceptive telemarketing acts or practices and other abusive telemarketing acts or practices).

59. See Federal Communications Commission, About Us, <http://www.fcc.gov/aboutus.html> (last visited Feb. 25, 2008).

60. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified in 47 U.S.C. § 151-710 (2007)).

data about a telephone subscriber to third-party advertisers for marketing purposes without the subscriber's consent, this will violate consumer privacy protections under the Telecommunications Act of 1996 ("Telecomm Act").<sup>61</sup> The FCC also enforces federal laws that restrict advertisers from making telephone calls using automated dialing systems.<sup>62</sup> Further, the FCC enforces the rules for making live advertising calls wireless telephone numbers.<sup>63</sup> Finally, the FCC is the primary administrative agency that regulates the sending of spam messages directly to wireless devices.<sup>64</sup> Recently, the FCC adopted new rules regulating telecommunications carriers that enhance consumers' data privacy and provide additional security protections related to subscribers' telephone records that include some sensitive forms of PII.<sup>65</sup>

Apart from the regulatory role of the FTC and the FCC, federal legislation governs eavesdropping, wiretapping, and accessing electronic records on the part of private businesses and governmental entities. This legislation is known as the Electronic Communications Privacy Act and is a source of privacy protection for mobile phone users.<sup>66</sup> Further, Congress recently passed a law that makes "pretexting" (obtaining telephone records by deception) a federal crime.<sup>67</sup> State and local governments may also protect consumers' privacy and personal data related to use of their mobile phones, unless preempted by federal law, although some states have

---

61. *Id.* However, the types of personal data protected by the Telecomm Act are limited and probably do not include cell phone numbers or other information that would normally be found in a telephone directory. *Id.*

62. See *infra* notes 160-165 and accompanying text.

63. 47 U.S.C. § 227(e); Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, *Rpt. and Order*, 18 F.C.C.R. 13013 (2003) (providing that the rules on initiating a telephone solicitation to residential telephone subscribers including restrictions on time of day that calls can be made and requiring the maintenance of a do-not-call list are applicable to any person or entity making telephone solicitations or telemarketing calls to wireless telephone numbers).

64. 15 U.S.C. § 7712 (2007) (regulating the sending of unwanted mobile service commercial messages, which addresses the sending or delivery of electronic commercial messages using a wireless Internet domain name found on an official list maintained by the FCC). See Edwin N. Lavergne, *FCC Gives Teeth to the CAN-SPAM Act of 2003, New Rules Strictly Limit Commercial Email to Cell Phones*, 1 N.Y.U. J. L. & BUS. 861, p.3 (2005). The FCC is required to consult with the FTC in the process of adopting administrative rules to regulate commercial spam sent to wireless devices). *Id.* at § 7712(b).

65. See ELECTRONIC PRIVACY INFORMATION CENTER. EPIC ALERT, June 14, 2007, [http://www.epic.org/alert/EPIC\\_Alert\\_14.12.html](http://www.epic.org/alert/EPIC_Alert_14.12.html) (reporting on the Federal Communication Commission's adoption of new rules to strengthen the security of consumers' phone records and its action seeking comments on possible additional steps it should take to protect the privacy of consumers).

66. 18 U.S.C. § 2510 (2000).

67. Telephone Records and Privacy Protection Act of 2006, 18 U.S.C. § 1039 (2007).

exempted mobile carriers from state consumer protection regulation.<sup>68</sup> It is common for state consumer protection laws to impose conflicting or more rigorous standards on advertisers than the standards imposed by federal law; for example, state law may prohibit telemarketing practices that are otherwise left unregulated by federal law.<sup>69</sup>

Finally, the common law of torts and the common law of contracts, often found in state court opinions rather than statutes or administrative law, are sources of state law remedies for privacy invasions involving mobile advertising. Contract law principles are particularly important to this Article's discussion of consumer privacy and the need for fair information practices for m-advertising. Whether an advertiser has provided adequate notice of its information practices or obtained appropriate consumer consent will often be determined by principles of contract law, including notions of assent necessary to form a binding contract and theories of implied-in-fact contracts. Because privacy protections based on common law tort and contract theories are a matter of state law, the applicable law may differ from state to state, adding complexity to this analysis. The next sections of this Article examine federal and state privacy laws to assess their adequacy to protect consumers' PII in the context of mobile advertising.

## V. FEDERAL PRIVACY REGULATION AND M-ADVERTISING

A complex web of federal regulation provides basic consumer privacy and data protection for mobile phone users and effectively limits mobile advertising practices. As this section of the Article describes, federal regulation may limit or prohibit mobile advertising practices that are unfair, deceptive, or otherwise present opportunities for privacy intrusions. Consumers also have some basic privacy protections under special laws that regulate the telecommunications industry and laws that restrict

---

68. FTC, Comments of Verizon Wireless In the Matter of Telemarketing Sales Rules Review, FTC File No. P994414, (May 16, 2006), *available at*: <http://www.ftc.gov/bcp/rulemaking/tsr/comments/verizon.htm> [hereinafter Verizon Comments on the TSR]. However, in some cases federal law preempts state and local law, limiting the powers of states in this regard. For example, the state of Washington has no power to regulate mobile carriers providing services to Washington residents. Press Release, Wash. Utils. Comm'n, Washington Regulators Adopt Nation's Strongest Telephone Customer-Privacy Rules (Nov. 7, 2002), *available at* <http://www.nfib.com/object/3577652.html> (stating that the WUTC rules apply to local and long-distance telecommunications companies providing service in Washington. The rules do not protect customers of wireless companies, because wireless companies are exempt from WUTC regulation).

69. See Verizon Comments on the TSR, *supra* note 68.

intercepting or accessing telephone and electronic communications.<sup>70</sup> Several key consumer privacy concerns are associated with m-advertising. As discussed in this section and summarized in Exhibit B, multiple forms of m-advertising raise consumer privacy concerns that are partially addressed by a patchwork of federal laws.<sup>71</sup>

**Exhibit B**

**Key Consumer Privacy Concerns Associated with Five Forms of Mobile Advertising—The Federal Regulatory Framework**

Key Consumer Privacy Concerns:	Forms of M-Advertisements:				
	Live Voice Solicitations to Mobile Phone Numbers	Autodialed Telemarketing Call to Mobile Phone Numbers	Electronic (Text, Multimedia, etc.) Message to Mobile Phone Numbers	.Mobi Ads on Web Sites Accessed Using Mobile Phones	Ads Generated by Adware on Cell Phone Handsets to Mobile Phone Subscribers
<b>Right to Prevent Disclosure of Wireless Phone Number for Marketing Purposes?</b>	No, FCC rule does not prevent carriers' disclosure, but violations of voluntary privacy policies may be unfair or deceptive practices.	No, but this type of telemarketing to wireless phone numbers is prohibited by FCC rule unless the called party has given express consent.	No, FCC rule does not prevent carriers' disclosure, but violations of voluntary privacy policies may be unfair or deceptive practices. <sup>72</sup>	No, not regulated except as unfair or deceptive trade practices.	No, not regulated except as unfair or deceptive trade practices (e.g., breach of privacy promise made in a company's privacy policy or deceptive downloading practices).
<b>Right to Give Consent Prior to Receiving Advertising?</b>	No	Yes, this type of telemarketing to wireless phone numbers is prohibited by FCC rule unless the called party has given prior express consent.	Yes, "opt-in" per CAN-SPAM for mobile spam sent using a wireless Internet Domain Name on the FCC's official list unless "transactional relationship exception" applies. CAN-SPAM's "opt-out" applies to mobile spam sent to wireless devices using	No, not regulated except as unfair or deceptive trade practice/ See privacy policy discussion above.	No, not regulated except as unfair or deceptive trade practices—see privacy policy discussion above.

70. See *supra* notes 59-61 (e.g., discussion of the Federal Communications Commission and the Telecommunications Act of 1996); see *infra* notes 246-267 (e.g., discussion of the Electronic Communications Privacy Act).

71. See *infra* Exhibit B: Key Consumer Privacy Concerns Associated with Five Forms of Mobile Advertising (discussing the Federal Regulatory Framework).



			other types of addresses (e.g. phone to phone SMS). <sup>73</sup>		
Right to "Opt-out" on the National Do-Not Call Registry?	Yes	Yes	Yes	No	No
Right to Make A Company-Specific Do Not Call Request?	Yes	Yes	Yes	No	No

As previously discussed, consumers also have some basic privacy protections under special laws that regulate the telecommunications industry, laws that restrict directing commercial advertising to mobile phones and laws that restrict intercepting or accessing telephone and electronic communications.

#### A. Breach of Privacy Policies as Unfair Trade Practices

The FTC prosecutes companies that violate their own consumer privacy policies under § 5 of the Federal Trade Commission Act ("FTC Act") that authorizes the FTC to protect consumers from unfair or deceptive acts or practices by businesses.<sup>74</sup> The FTC used its § 5 authority to prosecute Gateway Learning Corporation for breaching its privacy policy by renting its customers' personal information to other companies for advertising purposes. The rented information included customers' first and last names, home and mailing addresses, email addresses, phone numbers, and data about their past purchases.<sup>75</sup> Gateway's privacy policy promised not to sell, rent, or loan customers' PII to third parties without customers' express consent.<sup>76</sup> The companies that rented PII about

---

72. Mobile carrier's subscription agreement may not allow blocking to shield caller's number or may charge more to block caller identification. See Cingular Nation, Calling Plans (2007) (on file with author).

73. Opt-in rules for mobile advertising sent to a wireless device using a wireless Internet domain name listed on the FCC's official list are discussed *infra*, V.B.2. Opt-out rules apply to other advertising sent to mobile devices by technologies using other numbers and addresses (e.g. phone to phone text messages). See *infra*, V.B.1.

74. 15 U.S.C. § 57a(a)(1)(b) (2007) (providing FTC enforcement authority that covers unfair or deceptive acts or practices that occur in or affect interstate commerce). The FTC posts information regarding enforcement actions against companies that have breached their privacy policies on its Web site. See also Ciocchetti, *supra* note 56, at 72-74.

75. Agreement Containing Consent Order, Gateway Learning Corp., File No. 042-3047 (Fed. Trade Comm'n 2003), available at <http://www.ftc.gov/os/caselist/0423047/040707agree0423047.pdf>.

76. *Id.*

Gateway's customers used it to make telemarketing calls and to send direct mail solicitations to Gateway's customers.<sup>77</sup>

To date, the FTC's exercise of its § 5 enforcement powers to protect consumer privacy does not appear to deter abusive practices by advertisers, at least when it has not resulted in significant financial harm to consumers. The FTC's prosecutions of consumer privacy violators often result in agreements and consent orders that include promises by violators not to repeat the wrongdoing and the imposition of modest fines.<sup>78</sup> In the Gateway case, the company was required to disgorge approximately five thousand dollars obtained from renting customers' PII to advertisers—hardly an onerous sanction for a large and successful computer company like Gateway.<sup>79</sup> In contrast, when there is evidence of a privacy breach that has caused significant harm to consumers, FTC enforcement actions have garnered more significant civil remedies. For example, the FTC obtained a very large monetary settlement from ChoicePoint following its high profile investigation of data breaches resulting from ChoicePoint's failure to secure customers' PII.<sup>80</sup> The security breach at ChoicePoint resulted in over 800 cases of identity theft.<sup>81</sup> To settle the FTC's claims, ChoicePoint agreed to pay \$10 million in civil penalties and \$5 million in consumer redress.<sup>82</sup>

---

77. *Id.*

78. Some commentators believe that FTC prosecution fails to provide significant consumer protection because the FTC has discretion to refrain from prosecuting violations that are reported to it. Perceived weaknesses in the FTC's enforcement of § 5 include the FTC's standard investigation approach that involves negotiations with violators to obtain their promises to reform as opposed to seeking harsher sanctions for violations and the fact that the FTC cannot prosecute a company in the first place unless the company has taken the voluntary step of establishing a privacy policy that includes promises to protect consumers' privacy that the company has then breached. Hildner, *supra* note 29, at 145. However, the FTC has obtained substantial fines in some cases. *See generally* Federal Trade Commission, Enforcement, [http://www.ftc.gov/privacy/privacyinitiatives/promises\\_enf.html](http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html) (last visited Feb. 25, 2008). Further, agreements to resolve cases between the FTC and companies found to have violated their privacy policies have included consent orders requiring imposition of security procedures to protect consumers' PII and requiring third party audits of those procedures for up to twenty years. *Id.*

79. Press Release, FTC, Gateway Learning Settles FTC Privacy Charges (Jul. 7, 2004), available at <http://www.ftc.gov/opa/2004/07/gateway.htm>.

80. Press Release, FTC, ChoicePoint Settles Data Security Breach Charges; to Pay \$10 Million in Civil Penalties, \$5 Million for Consumer Redress (Jan. 26, 2006), available at <http://www.ftc.gov/opa/2006/01/choicepoint.htm>.

81. *Id.*

82. *Id.* *See also* Roy Mark, *ChoicePoint ID Theft Victims' Day Has Come*, INTERNETNEWS.COM (Dec. 7, 2006), <http://www.internetnews.com/bus-news/print.php/3647631> (reporting that victims of the ChoicePoint identity theft scandal have been mailed claims forms by the FTC to seek recovery of out-of-pocket expenses from the \$5 million fund established by the settlement of FTC claims against ChoicePoint).

Administrative agency discretion also plays a role in the deterrent effect of FTC enforcement to protect consumer privacy. When new technologies emerge that may have privacy-intrusive applications, the FTC has discretion to decide whether it will regulate the use of the technologies or choose instead to refrain from such regulation and encourage industry self-regulation in order to allow the technology to expand. This approach arguably allows industries that develop new technologies to mature free of the risk of excessive government regulation. Initially, the FTC took this approach with respect to regulating the use of adware and spyware—technology that also generates personal data protection and privacy issues for consumers.<sup>83</sup> However, the FTC reversed its nonenforcement position recently when it took action against deceptive practices by firms that deploy adware and spyware as well as against companies that have hired other firms to deliver advertising using adware and spyware.<sup>84</sup> The FTC also acknowledged that new federal legislation to protect consumers from invasive uses of adware and spyware is needed. The inclusion of GPS and RFID technologies in mobile phones will enable advertisers to target mobile phone users with personalized location-based advertising, raising new consumer privacy issues. However, consistent with its initial position regulating adware and spyware, the FTC has elected not to issue any guidelines on the use of RFID by companies but rather to allow the technology to develop and allow companies that use RFID a chance to regulate themselves on matters of consumer privacy.<sup>85</sup>

---

83. PATRICIA MOLONEY FIGLIOLA, CONGRESSIONAL RESEARCH SERVICE, *SPYWARE: BACKGROUND AND POLICY ISSUES FOR CONGRESS* (2006) (discussing adware and spyware technologies that may be deployed by distributors without appropriate user consent and implemented in ways that impair users' control over their computer systems and the collection, use, and distribution of users' PII) [hereinafter CRS Report for Congress on Spyware]. Spyware is not a well-defined term but is generally used to refer to any software that is downloaded onto a user's computer without his or her knowledge; types of spyware include "key-logging" software that records the user's keystrokes (may include passwords and other sensitive information), software that monitors Web browsing habits, and software that may relay user's personal information to another computer. Adware includes software that may cause advertisements to suddenly appear on the user's monitor (pop-up ads). *Id.*

84. *Id.* (reporting that in 2005, the FTC initiated five law enforcement actions related to spyware and supported legislation that would enhance its ability to seek penalties against spyware distributors and to investigate and prosecute spyware distributors that are located abroad or who use foreign intermediaries). See also Cindy Skrzycki, *Stopping Spyware at the Source*, WASH. POST, Mar. 6, 2007, at D1 (reporting settlements obtained by the FTC in investigations of deceptive advertising cases brought against distributors of adware or spyware for using deceptive methods to get consumers to download their advertising software that tracks computer use and generates pop-up ads) (also reporting a settlement between the New York Attorney General and Cingular Wireless, Travelocity.com, and Priceline.com following the state's investigation of these companies use of a spyware distributor to deliver advertisements for the companies).

85. See Jonathan Collins, *FTC Asks RFID Users to Self-Regulate*, RFID J., Mar. 10, 2005, <http://www.rfidjournal.com/article/view/1437/1/1/>; FTC RFID Workshop Report,

Beyond the FTC’s general enforcement powers under § 5, specific federal statutes have been enacted that give federal agencies like the FTC and the FCC authority to regulate abusive advertising practices that involve sending unsolicited advertisements via email or text messages (“spam”) and making telemarketing calls to consumers. These regulations address specific forms of unfair or deceptive advertising practices that implicate consumer privacy and set minimum standards of conduct for mobile advertisers to protect consumer privacy. Exhibit C analyzes the federal regulatory framework that governs mobile advertising solicitations and summarizes the federal laws that may require m-advertisers to provide privacy notices to consumers and obtain consumers’ consent to receive advertising solicitations.

**Exhibit C**  
**Required Notice and Consent for Mobile Advertising Solicitations**  
**The Federal Regulatory Framework**

	Form of Notice	Level of Consumer Consent	Exceptions	Consumer Remedy for Violations?
<b>Commercial Message Sent Directly to a Mobile Phone<sup>86</sup></b>	Sender must provide notice and request consent before sending message ads directly to mobile phones (e.g., text, email, multimedia) . Notice must include the name of sender or advertiser (if differs from sender) and information on how to revoke consent.	Express pre-authorization (“opt-in”) in written, oral or electronic form must be obtained from subscriber . Request for authorizations must be conveyed at no additional cost to consumer and consumer must be able to reply at no additional cost. Authorization by consumer must include the email address where MSCMS can be sent.	Transactional or relationship messages (primary purpose is to facilitate a business transaction or to provide warranty, product recall, safety, or security information to the consumer) do not require “opt-in” notice and consent.	No, File FCC Complaint  CAN-SPAM does not permit the consumer to sue the violator for civil remedies.
<b>Commercial Message Accessed through a</b>	“Opt-out” notice required that complies with CAN-SPAMs	Subscriber pre-authorization not required (unless “opt-out” request	Transactional or relationship messages may be sent, even if an “opt-	No, File FTC Complaint.  CAN-SPAM does not

*supra* note 47. Of course, in the future the FTC could change its position on enforcing the FTC Act relative to RFID and consumer privacy issues. The European Commission has also determined that the time is not yet ripe to adopt rules regulating RFID technologies, although a top official warned that regulations are likely if future uses of the technology don’t protect fundamental privacy rights. Anne Broache, *E.U. Official: Now Isn’t Time for RFID Regulations*, CNET NEWS.COM (Apr. 2, 2007), [http://www.news.com/2100-1029\\_30612675.html](http://www.news.com/2100-1029_30612675.html).

86. Before sending Mobile Service Commercial Messages (MSCM) (defined as a message sent directly to a mobile phone using a wireless Internet Domain Name on the FCC’s official list) advertisers must give specific notices to consumers and obtain their express authorization. *See* discussion and references at *supra* notes 120-132.

<b>Mobile Phone (Non-MSCM Ad Messages)</b> <sup>87</sup>	rules—sender of text, email, multimedia commercial solicitation message, etc. must honor “opt-out” request w/n 10 business days.	has been previously made) by the consumer).	out” request has been made	permit the consumer to sue the violator for civil remedies (but see state anti-spamming laws).
<b>Live Telemarketing Call to Mobile or Landline Phone Number</b>	“Opt-out” notice unless number is listed on National DNC Register Telemarketing Sales Rule and its requirements for disclosures apply, e.g., sender must state the purpose of the call.	Subscriber pre-authorization to make the call not required unless subscriber’s phone number is on National DNC Register or has made Company-specific DNC request.	Established Business Relationship exception allows advertiser to call a subscriber on the National DNC register if caller has such a relationship with the subscriber and subscriber has not made a company-specific DNC request.	Yes, consumers may sue TCPA <sup>88</sup> violators for the greater of \$500 for each violation or actual damages, with the possibility of recovering treble damages.
<b>Auto-dialed Telemarketing Call to Mobile Phone Number</b>	“Opt-in” notice (without preauthorization, such calls are prohibited if made to mobile phones)	Prior Express Consent of Called Party Required	No Established Business Relationship exception	Yes, consumers may sue TCPA violators for the greater of \$500 for each violation or actual damages, with possible recovery of treble damages.

### B. *Spamming as an Unfair Trade Practice*

The federal spamming law applies to m-advertising to the extent that communications of mobile advertising messages fit within the law’s definition of “commercial electronic communications.”<sup>89</sup> The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (“CAN-SPAM”) covers commercial electronic communications sent to recipients in the U.S.<sup>90</sup> CAN-SPAM prohibits false or deceptive spamming practices such as using false or misleading information in email headers, including deceptive subject lines in email messages, or failing to include senders’ functioning return email addresses.<sup>91</sup> It is unlawful to send unsolicited commercial electronic messages that do not include: clear and

87. See discussion of “opt-out” rules for m-ads that are not Mobile Service Commercial Messages (MSCM), *supra* notes 115-119. For example, if a m-advertiser sends an ad to the mobile phone owner’s email account at yahoo.com, this is not a MSCM, because to do so does not require using a wireless Internet domain name on the FCC’s official list. See FCC, Consumer & Governmental Affairs Bureau, CAN\_SPAM: Unwanted Text Messages and E-Mail on Wireless Phones and Other Devices, at: <http://www.fcc.gov/cgb/consumerfacts/canspam.html>.

88. See discussion of remedies under the Telephone Consumer Protection Act (TCPA), *supra* note 149

89. 15 U.S.C. § 7702 (2007).

90. *Id.*

91. *Id.*

conspicuous identification that the messages are advertisements or solicitations; clear and conspicuous notice of the recipients' opportunity to "opt-out" of receiving further messages from senders; and valid physical postal addresses of the senders.<sup>92</sup> CAN-SPAM requires senders of unsolicited commercial electronic messages to honor "opt-out" requests within ten business days.<sup>93</sup> The provisions of CAN-SPAM apply to a communication sent to a single address as well as mass mailings to multiple recipients. The law covers commercial electronic messages sent to businesses as well as consumers.<sup>94</sup> Further, the law prohibits businesses from knowingly using a third party to send commercial electronic messages that violate CAN-SPAM.<sup>95</sup>

Not all commercial electronic communications get the same level of regulation under CAN-SPAM. Transactional or relationship messages that have a primary purpose of facilitating, completing, or confirming a commercial transactions are excluded from most of the form and disclosure requirements of CAN-SPAM. Transactional or relationship messages include messages sent by businesses to their customers containing warranty information, product recall information, or safety and security information about their products or services.<sup>96</sup>

The FTC has adopted final administrative regulations interpreting CAN-SPAM.<sup>97</sup> One purpose of the regulations is to clarify when a commercial electronic message has a primary purpose that is commercial, thus distinguishing this type of message (which must comply with all of the

---

92. 15 U.S.C. § 7704(a)(5).

93. 15 U.S.C. § 7704(a)(4).

94. 15 U.S.C. § 7702(2) (defining commercial electronic mail messages as 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). The term recipient when used with respect to a commercial electronic message means an authorized user of an electronic mail address. 15 U.S.C. § 7702(14). Such a recipient is not limited to a consumer so by implication includes businesses as well as consumers. *Id.*

95. 15 U.S.C. § 7705(b) (providing liability for the third party's actions in violation of CAN-SPAM). The FTC has exclusive enforcement powers related to imputed third party liability for violations of CAN-SPAM. 15 U.S.C. § 7705(c). *See also* United States v. Cyberheat, Inc., No. 05-457, 2007 WL 686678, at \*1 ( D. Ariz., 2007) (holding that an advertiser may be held vicariously liable for a marketing partner's CAN-SPAM Act violations, including sending sexually explicit email to consumers without conforming to the requirements of CAN-SPAM or obtaining consumers' consent, if the advertiser had the ability to control the actions of the partner and knew or should have known that the partner was violating the law).

96. 15 U.S.C. § 7702(17).

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

CAN-SPAM requirements) from transactional messages.<sup>98</sup> Transactional messages are only required to have accurate header information but need not comply with other CAN-SPAM requirements such as the inclusion of “opt-out” privacy notices.<sup>99</sup> The final regulations also address CAN-SPAM’s requirement that sexually-oriented commercial electronic messages be specifically labeled—for example, an email message containing sexually explicit materials must include the words “SEXUALLY-EXPLICIT” in the subject line of the email.<sup>100</sup> After studying the issue, the FTC decided not to recommend the establishment of a Do-Not-Email Registry, having concluded that such a register would likely become a preferred list of working email numbers that would be used by spammers to generate spam rather than working as an effective tool to restrict spam and protect the privacy of email users.<sup>101</sup>

CAN-SPAM does not give consumers the right to sue spammers for damages.<sup>102</sup> However, consumers may file complaints against spammers with the FTC, and the FTC has discretion to pursue civil remedies against spammers.<sup>103</sup> In addition to FTC enforcement, state governments and Internet Access Providers (“IAP”) may also enforce CAN-SPAM and

---

98. *See id.*; *see generally* Susan Kuchinskas, *FTC Closing CAN-SPAM Loopholes*, INTERNETNEWS.COM (Jan. 28, 2005), [www.internetnews.com/ec-news/article.php/3465931](http://www.internetnews.com/ec-news/article.php/3465931).

99. Press Release, FTC, *FTC Postpones Effective Date of CAN-SPAM Rule Establishing Criteria for Determining “Primary Purpose” of E-Mail Messages* (Jan. 12, 2005), *available at* <http://www.ftc.gov/opa/2005/01/primarypurp.htm> (summarizing the criteria for determining whether the primary purpose of an email is commercial, as set forth in the final rule adopted by the FTC).

100. Press Release, FTC, *FTC Adopts Rule That Requires Notice that Spam Contains Sexually-Explicit Material* (Apr. 13, 2004), *available at* <http://www.ftc.gov/opa/2004/04/adultlabel.htm> (characterizing this rule as a “brown-paper wrapper” requirement for sexually-oriented material sent in unsolicited commercial electronic mail).

101. *See* FEDERAL TRADE COMMISSION, *EFFECTIVENESS AND ENFORCEMENT OF THE CAN-SPAM ACT*, app. 3 (December 2005) *available at* <http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf> [hereinafter Report to Congress on CAN-SPAM]. *But see* the FCC’s official register of wireless Internet domain names *available at*: [www.fcc.gov/cgb/policy/DomainNameDownload.html](http://www.fcc.gov/cgb/policy/DomainNameDownload.html) (providing FCC-required listing by all wireless service providers of all Internet names used to transmit electronic messages directly to wireless devices). Senders have 30 days from the date a wireless Internet domain name is posted on the FCC site to stop sending unauthorized commercial email and other electronic messages to Internet addresses containing the listed domain name. *Id.*

102. However, some state antispam laws allow consumers to sue for damages. For example, the state of Washington has a plaintiff-friendly antispam law which allows most people to sue to \$500 in damages per unsolicited message. A person who qualifies as a provider of Internet access to other people may recover \$1000 in damages per message. WASH. REV. CODE § 19.190.040 (2007). *See* Declan McCullagh, *Lawsuit Shows How to Sue Spammers*, CNET NEWS.COM (June 20, 2007), [http://www.news.com/2100-1030\\_3-6192208.html](http://www.news.com/2100-1030_3-6192208.html).

103. *See* FTC, *FTC Consumer Complaint Form*, [https://m.ftc.gov/pls/dod/wsolcq\\$.startu?p?Z\\_ORG\\_CODE=PU01](https://m.ftc.gov/pls/dod/wsolcq$.startu?p?Z_ORG_CODE=PU01) (last visited Nov. 21, 2007). This Web site also allows consumers to forward unsolicited commercial email to the FTC without filling out a complaint form.

recover damages.<sup>104</sup> Spammers face both civil and criminal penalties for violating CAN-SPAM. Civil penalties include recovery of statutory damages (up to \$250 for each separately addressed unlawful email), treble damages for willful and knowing violations, and costs of the action and reasonable attorneys' fees.<sup>105</sup> The amount of statutory damages recoverable by an IAP under CAN-SPAM is lower than that recoverable by the state government or the federal government—statutory damages recoverable by an IAP range from \$25-\$100 per unlawful email but may not exceed \$1 million.<sup>106</sup> Spammers may also be criminally prosecuted under CAN-SPAM. Criminal penalties for spammers include sentences ranging from two to five years for each offense.<sup>107</sup>

Despite numerous civil and criminal actions against spammers<sup>108</sup>—some of whom have received lengthy prison terms and hefty fines<sup>109</sup>—unsolicited junk email has increased since CAN-SPAM was enacted, and some spammers have moved outside the U.S. to minimize the likelihood of being prosecuted under CAN-SPAM.<sup>110</sup> In response, the FTC Act was amended by the Safe Web Act of 2006 to give the FTC stronger powers to protect consumers from spam, spyware, and other forms of Internet fraud and deception.<sup>111</sup> The FTC now has increased authority to share

---

104. 15 U.S.C. § 7706(f) (2006).

105. *Id.*

106. 15 U.S.C. § 7706(g) (2006). Any party in action for damages brought by an IAP may be required to pay the other party the costs of the action and reasonable attorneys' fees. 15 U.S.C. § 7706(g)(4).

107. *See, e.g.*, 15 U.S.C. § 7704(1)-(5) (providing prison for five years for knowingly failing to place on unsolicited commercial email the required warning label that it contains sexually-oriented material content).

108. Report to Congress on CAN-SPAM, *supra* note 101, at app. 5-7. *See also*, *Gene Johnson, Man Described as a Top Spammer Arrested*, WASHINGTON POST, at B1 (May 31, 2007), available at [http://www.washingtonpost.com/wpdyn/content/article/2007/05/30/AR20\\_07053002515.html?tid=informbox](http://www.washingtonpost.com/wpdyn/content/article/2007/05/30/AR20_07053002515.html?tid=informbox) (reporting on the arrest in the U.S. of a man who is reportedly one of the "top 10 spammers in the world").

109. *See Kodak Pays Up Over Spam Charges*, ZDNET.CO.UK, May 11, 2006, <http://news.zdnet.co.uk/itmanagement/0,1000000308,39268536,00.htm> (reporting that Kodak paid over \$26,000 to the FTC to settle charges that it sent emails to two million recipients and failed to give them a way to opt out of future messages, a violation of CAN-SPAM); *see also* Associated Press, *21-Year-Old Hacker Sentenced to Nearly 5 Years in Prison*, May 09, 2006, available at <http://www.foxnews.com/story/0,2933,194860,00.html> (reporting that the conviction was for a felony related to taking control of 400,000 Internet-connected computers and renting access to them to spammers and fellow hackers).

110. *See* Brad Stone, *Spam Doubles, Finding New Ways to Deliver Itself*, N.Y. TIMES, Dec. 6, 2006.

111. Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers Beyond Borders Act of 2006, Pub. L. No. 109-455, 120 Stat. 3372 (2006) [hereinafter *Safe Web Act*]. The Safe Web Act authorizes the FTC to share information with criminal authorities, including providing investigative assistance for foreign law enforcement agencies, sharing information with foreign agencies that prosecute consumer fraud and deception as a criminal



information with foreign agencies that prosecute spammers and other forms of consumer fraud as well as to participate in foreign litigation.<sup>112</sup>

Enforcement power under CAN-SPAM is shared by the FTC and FCC. The FCC is responsible for regulating commercial electronic messages sent directly to mobile phone subscribers, and the FTC is responsible for regulating other forms of commercial electronic messages, including email spam accessed using, but not sent directly to, mobile phones.<sup>113</sup> Accordingly, the FCC has regulated unsolicited commercial electronic mail sent to *wireless* devices.<sup>114</sup> The distinction between sending covered spam directly to a mobile phone subscriber and sending it to a source that is accessed by a subscriber using a mobile phone is important. This distinction determines whether the advertiser must obtain the consumer's consent before sending an electronic advertising message to the consumer or may instead rely on "opt-out" consent mechanisms.

### 1. "Opt-out" Consent is the Minimum Required to Send Unsolicited Advertising Accessed on Mobile Phones

Generally speaking, marketers may send unsolicited commercial electronic messages (e.g., unsolicited email advertisements or advertising "spam") to consumers and businesses without obtaining the advance consent of the recipients as long as: 1) the messages conform to the requirements of CAN-SPAM (e.g., not false or deceptive, form requirements met, etc.), 2) the messages are not sent directly to mobile phone subscribers (Mobile Service Commercial Messages or MSCMs, discussed in the next section), and 3) the recipients have not "opted-out" of receiving these types of commercial electronic messages from the sender.<sup>115</sup> Senders are required to notify recipients that they may elect not

---

law enforcement issue, and permitting the FTC to work with the U.S. Department of Justice to increase resources related to FTC-related foreign litigation, including freezing foreign assets and enforcing U.S. court judgments in foreign countries. *Id.* at § 4-6.

112. *Id.*

113. CAN-SPAM gives the FCC the power to enforce the provisions of CAN-SPAM with respect to any person subject to the provisions of the Telecomm Act. 15 U.S.C. § 7706(b)(10) (2006). CAN-SPAM gives the FTC the power to enforce the provisions of CAN-SPAM under its statutory authority to enforce unfair or deceptive acts or practices. 15 U.S.C. § 7706(a). A violation of CAN-SPAM by a person regulated by the FCC is deemed to be a violation of a Federal Trade Commission trade regulation rule. 15 U.S.C. § 7706(c).

114. 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, 47 C.F.R. Part 64.3100, FR 55765-01 [hereinafter FCC's Mobile Spam Regulations].

115. 15 U.S.C. § 7704. See also FTC, FTC FACTS FOR BUSINESS: THE CAN-SPAM ACT: REQUIREMENTS FOR COMMERCIAL EMAILERS, (Apr. 2004), available at <http://www.ftc.gov/bcp/online/pubs/buspubs/canspam.pdf>. Consumers also have the ability to "opt-out" from receiving commercial electronic telephone calls (voice or text messages) on their

to receive future email messages (by making “opt-out” requests to senders) and senders are required to honor recipients’ “opt-out” requests.<sup>116</sup> CAN-SPAM’s general process of allowing advertisers to send unsolicited email communications to consumers, as long as the consumer has not made a request not to receive such communications, establishes an “opt-out” process of obtaining consumer consent.<sup>117</sup> In contrast, an “opt-in” process of obtaining consumers’ consent requires the sender to obtain consent from the consumer before sending them even one electronic advertisement.<sup>118</sup>

CAN-SPAM’s “opt-out” consent rules apply to unsolicited commercial electronic messages (e.g., email, text, or instant messages) sent to consumers, including those accessed by consumers using their mobile phones, provided the advertiser has not sent the advertising messages directly to an wireless Internet domain name listed on the FCC’s official list, as discussed in the next section. For example, because the domain name yahoo.com is not on the FCC’s official list of wireless Internet domain names registered to mobile carriers, an advertiser may send an advertising email message to “consumer@yahoo.com” without first obtaining the consumer’s advance authorization. This is so even if the consumer later accesses the email message from yahoo.com using his mobile phone. Additionally, an advertiser may use a cell phone to send a text message to a consumer using the consumer’s mobile phone number, a so called “phone to phone” text message, as long as the consumer has not listed their phone number on a do-not-call registry and the advertiser is not using autodialing equipment to generate the call (see Section V.C.).

However, as described in the next section, an advertiser must obtain the consumer’s express authorization in advance (“opt-in” notice and consent) before sending certain types of commercial electronic messages directly to consumers’ mobile phones—MSCMs.

## 2. “Opt-in” is Required to send M-Ads Directly to Mobile Phones Using MSCMs

The FCC, as opposed to the FTC, primarily enforces Section 14 of CAN-SPAM with respect to sending MSCMs and the FCC may impose penalties of up to \$10,000 for each violation.<sup>119</sup> Generally speaking,

---

wireless phones by registering their mobile phone numbers on the National Do Not Call Registry. See *infra* Section V.C.1. Further, some telemarketing practices, such as using autodialing telephone equipment to generate telemarketing calls, is limited by federal law. *Id.*

116. *Id.*

117. 47 C.F.R. § 64.2003(h).

118. *Id.*

119. See *supra* notes 59-65 and accompanying text. The CAN-SPAM Act required the FCC to issue rules with regard to commercial electronic messages such as email, text

MSCMs are electronic communications that contain advertising messages that are sent directly to mobile phones via the Internet. A MSCM is defined as a commercial electronic mail message transmitted *directly* to a wireless device utilized by a subscriber of commercial mobile service (e.g., a cell or mobile phone subscriber) in conjunction with that service.<sup>120</sup> To ensure that advertisers have the ability to distinguish when an advertising message that is to be sent will be covered by the MSCM rules, the FCC publishes lists of wireless Internet domain names on its Web site (FCC official list).<sup>121</sup>

Any one with an Internet email account and knowledge of a mobile phone subscriber's mobile telephone number can send an electronic message to the subscriber using a domain name provided by the subscriber's mobile carrier—for example, send an email to a mobile subscriber (using one of these domain names and inserting the subscriber's 10 digit mobile phone number to create an electronic address for the subscriber) that will be delivered as a text or multimedia message on the subscriber's mobile phone.<sup>122</sup> So, were it not for CAN-SPAM's restrictive

---

messages, etc. sent directly to wireless devices and authorized the FTC to issue rules with respect to commercial electronic messages other than that sent directly to wireless devices. See FCC, CAN-SPAM, Unwanted Commercial Electronic Mail, <http://www.fcc.gov/cgb/policy/canspam.html> (last visited Feb. 18, 2008). Specifically, § 14 of the CAN-SPAM Act requires the FCC to develop rules to protect consumers from "unwanted mobile service commercial messages." *Id.* Civil penalties up to \$10,000 per violation may be imposed by the FCC on violators. 15 U.S.C. §45(m)(1)(A).

120. See Lavergne, *supra* note 64, at 861. 15 U.S.C. § 7712(d) (referencing 47 U.S.C. § 332(d) for the definition of commercial mobile service). In this paper, the term "mobile spam" is used to refer to commercial advertising solicitations made to mobile phone subscribers or delivered to mobile phones, but it is a broader term than MSCM, because the latter is limited to m-ads sent to or delivered using wireless Internet domain names. For example, the FCC's ban on sending commercial messages to wireless devices "does not cover 'short messages' [text messages] sent from one mobile phone to another if to do so does not use an Internet address" listed on the FCC's official list. See FCC, CAN-SPAM, Unwanted Commercial Electronic Mail, <http://www.fcc.gov/cgb/policy/canspam.html> (last visited Mar. 11, 2008). However, if a text message advertisement is generated using automated dialing equipment, this would be prohibited by the TCPA. See 2003 TCPA Order, *infra* note 152, at para. 165.

121. 47 C.F.R. § 64.3100(a)(4) (2006). The list of wireless mail domain names is available on the FCC's Web site. See FCC, Consumer Policy Issues, <http://www.fcc.gov/cgb/policy/DomainNameDownload.html> (last visited Feb. 18, 2008) [hereinafter FCC official list]. This domain name list is updated when wireless service providers submit valid domain names or delete unused domain names. Wireless service providers are required to update the list not less than thirty days before issuing subscribers any new or modified domain name and to remove any domain name that has not been issued to subscribers or is no longer in use within six months after placing it on the list or its last date of use. *Id.* Advertisers must consult the FCC's official list before sending email and other electronic advertising to consumers—if an address on the advertiser's mailing list includes a wireless Internet domain name on the FCC's official list, the advertiser is not permitted to send advertising to the address without obtaining the recipient's express prior consent. *Id.*

122. *Id.* See Lavergne, *supra* note 64, at 861. See, e.g., AT&T Wireless (formerly Cingular Wireless), What is the E-Mail Address for Text Messaging, Multimedia

rules that make it unlawful to send commercial advertising messages in this manner unless the sender has the recipient's prior express consent, it would be very easy for advertisers to send m-ads to mobile phone subscribers to be delivered as text or multimedia messages on subscribers' mobile phones. Because advertisers that generate electronic messages to consumers via the Internet are not making telephone calls in the traditional sense, existing laws regulating telemarketing would not apply and having previously listed one's mobile phone number on the National Do Not Call Registry would not prevent the sending of MSCMs. Essentially, the more restrictive FCC rules under CAN-SPAM that apply to sending MSCMs are designed to protect mobile phone subscribers from receiving this type of mobile spam unless they have given their consent.

To lawfully send MSCMs to mobile phone subscribers, advertisers must first obtain their *express authorization*—"opt-in consent."<sup>123</sup> However, there is an exception to the requirement of "express prior authorization" for transactional or relationship messages. Transactional or relationship messages sent to mobile phones include electronic messages that have the primary purpose of facilitating a business transaction or providing warranty, product recall, safety, or security information to consumers.<sup>124</sup>

The FCC's administrative rules implementing CAN-SPAM specify that "express prior authorization" to send MSCMs may be written, oral, or electronic.<sup>125</sup> If there is a dispute between the sender and recipient as to

Messaging, Xpress Messaging, RIM BlackBerry and Media Net? [hereinafter AT&T, What is the E-Mail Address for Text Messaging, etc.?], <https://cingular.atgnow.com/cng/tutorials/KB45161.html> (last visited Feb. 25, 2008). To generate a text message to a subscriber with ATT's wireless service, the sender sends an email message from any Internet email account to subscriber at the address that includes the subscriber's ten digit mobile phone number, e.g., "10digitmobilenumber@txt.att.net". *Id.* The sender does not need to know any information except the recipient's mobile phone number in order to generate this email directed at a mobile phone. *Id.* The recipient will receive the email as a text message (SMS) and will generally be billed for the receipt of the message. *Id.*

123. 15 U.S.C. § 7712(b)(1).

124. 47 C.F.R. §§ 64.3100(c)(2), (8). However, advertisers are prohibited from obtaining express authorization from consumers by sending a request to a consumer using one of the wireless Internet domain names on the FCC's list, or doing so in a way that would result in a cost to the consumer. *See* Lavergne, *supra* note 64. However, the advertiser may use a postcard, telephone call or a Web site to obtain express consent to send MSCM. *Id.*

125. 47 C.F.R. §§ 64.3100(a), (d). *See generally* Fed. Rules and Regs. Implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, *Order*, 19 F.C.C.R. 15927 (2004). Required disclosures must be made by the advertiser to the consumer in order to obtain express prior authorization; these disclosures include telling the consumer the identity of the sender (and advertiser, if different) who will be sending the MSCS and telling the consumer of his right to revoke his consent at any time. *Id.* p.7. There are also limitations on the scope of the subscriber's consent, for example:

A subscriber who provides an electronic mail address for a specific purpose, e.g., notifying the subscriber when a car repair is completed, will not be considered to

whether the recipient gave express prior authorization, the sender has the burden to demonstrate that the recipient expressly authorized the sending of commercial electronic communications to a mobile phone.<sup>126</sup>

The FCC's new rules apply only to "commercial electronic mail messages," which is defined as any electronic mail message whose "primary purpose . . . is the commercial advertisement or promotion of a commercial product or service (including content on an Internet Web site operated for a commercial purpose)."<sup>127</sup> The FCC's official list of wireless domain name registers is functionally equivalent to a national Do Not E-Mail list, with the exception that carriers list the domain names, rather than subscribers listing their mobile phone numbers, and it avoids creating a list of working electronic addresses for mobile subscribers that could be used by spammers to generate mobile spam.<sup>128</sup>

On the whole, the wireless industry claims not to have had many problems with unsolicited wireless messages because wireless carriers recognize that they have a strong incentive to protect customers from unwanted messages.<sup>129</sup> "To capture the huge potential of wireless data

---

have given express prior authorization for purposes of sending MSCMs in general. In addition, should a sender allow subscribers to choose the types of MSCMs they receive from that sender, and authorization is provided for those specific types of messages, the sender should transmit only those types of MSCMs to the subscriber. Finally, authorization provided to a particular sender will not entitle the sender to send MSCMs on behalf of third parties, including on behalf of affiliated entities and marketing partners.

*Id.* at p.8.

126. Rules and Regs. Implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 69 Fed. Reg. 55765, 55770 (codified at 47 C.F.R. pt. 64) (noting that "in the event any complaint is filed, the burden of proof rests squarely on the sender, whether authorization has been obtained in written or in oral form").

127. 47 C.F.R. § 64.3100(c)(2); 15 U.S.C. § 7702(2)(A). The FTC has also promulgated rules to address when the primary purpose of an electronic communication is advertisement or promotion, and these rules apply to advertising sent directly to wireless devices as well as that delivered using other forms of electronic communications. 47 C.F.R. § 64.3100(c)(2). See generally Final Rule, Definitions and Implementation under the CAN-SPAM Act, *supra* note 97.

128. 47 C.F.R. § 64.3100(e)(requiring CMRS to identify all electronic mail domain names used to offer subscribers messaging specifically for wireless devices in connection with commercial mobile service for the FCC's official list). See Final Rule, Definitions and Implementation under the CAN-SPAM Act, *supra* note 97, at 4-6. It is a safe-harbor defense to prove that a specific domain name was not on the FCC's official list more than 30 days before the offending message was initiated, however this defense does not excuse a person who knowingly initiated a message to a mobile subscriber, even if it is sent within 30 days of the domain name appearing on the list. *Id.* at 5.

129. Michael F. Altschul, Senior Vice President and General Counsel, Cellular Telecommunications & Internet Association, Before the Federal Trade Commission, "SPAM Forum" (May 1, 2003), available at <http://www.ftc.gov/bcp/workshops/spam/Supplements/altshcul.pdf> [hereinafter Altschul Remarks]; see also Comments of AT&T Wireless on Short Messaging Service Spam, Federal Trade Commission Spam Forum (April

services, carriers must convince customers to upgrade to handsets and devices that support these services and features, and then to use these services. If spam ruins the user [s' mobile] experience, the opportunity of wireless data will be lost."<sup>130</sup> To further protect users' wireless experiences, two mobile phone companies recently joined in a lawsuit to stop spam being sent by telemarketers using their cellular networks.<sup>131</sup> In the same vein, Verizon Wireless recently reported that it sued a wireless spammer and won a default judgment against the wireless spammer, barring it from sending future spam text messages to its wireless customers and ordering the spammer to pay over \$200,000 in damages to Verizon.<sup>132</sup>

### C. Telemarketing as Unfair Trade Practices

As in the case of the regulation of mobile spam, the FTC and the FCC both regulate telemarketing practices that target mobile phone users.

#### 1. The Telemarketing Sales Rule

The FTC has statutory authority to protect consumers from unfair and deceptive telemarketing practices, including telemarketing calls made to mobile phones.<sup>133</sup> The FTC has adopted final administrative rules under this statutory authority that prohibit telemarketers from undertaking patterns of unsolicited advertising calls that a reasonable consumer would consider coercive or abusive to his or her right to privacy.<sup>134</sup> These rules also restrict the hours of the day and night when unsolicited telephone calls

---

30-May 2, 2003), available at <http://www.ftc.gov/bcp/workshops/spam/Supplements/attwireless.pdf>.

130. Altschul Remarks, *supra* note 129, at 2.

131. Sheri Qualters, *Cingular and Verizon Wireless Join Forces Against Cell Phone 'Spam'*, LAW.COM, Nov. 6, 2006, <http://www.law.com/jsp/article.jsp?id=1162548321882>. Three federal lawsuits have been filed by Cingular and Verizon against telemarketers in an Atlanta federal court claiming that the telemarketers violated federal telephone consumer protection laws by sending spam to their cell phone customers and that defendants' unauthorized use of cellular networks to send the spam is conversion and unjust enrichment. *Id.*

132. Marguerite Reardon, *Verizon Wireless Wins Injunction Against Text Spam*, CNET NEWS.COM, Feb. 26, 2007, [http://www.news.com/2100-7350\\_3-6162263.html](http://www.news.com/2100-7350_3-6162263.html).

133. 15 U.S.C. § 6102 (2001) (empowering the FTC to prescribe rules prohibiting deceptive telemarketing acts or practices and other abusive telemarketing acts or practices). See also, *supra* notes 59-65, 120-128 and accompanying text for a discussion of the FCC's responsibility to regulate commercial solicitations sent to mobile phones.

134. See generally Telemarketing Sales Rule; Final Rule, 16 C.F.R. Part 310 (Jan. 29, 2003), available at <http://www.ftc.gov/os/2003/01/tsrfrn.pdf>. See also FTC, Telemarketing Sales Rule, Index of Rulemaking Record for the Final Amended Rule, <http://www.ftc.gov/bcp/rulemaking/tsr/tsrrulemaking/index.htm> (last visited Jan. 14, 2008). Charitable solicitors making telemarketing phone calls are also regulated under the Telemarketing Sales Rules. For example, charitable solicitors must disclose to recipients that the purpose of their telemarketing calls is to solicit charitable donations. 16 C.F.R. § 310.4(e)(2007).

may be made to consumers and require that telemarketers disclose the purpose of their calls, including telling consumers that the object of the calls is to sell goods or services.<sup>135</sup> These lengthy administrative rules are known as the Telemarketing Sales Rule.<sup>136</sup>

*National Do Not Call Registry:* Under the Telemarketing Sales Rule, telemarketers are prohibited from making telemarketing calls to consumers' telephone numbers that are listed on the National Do Not Call Registry.<sup>137</sup> Telemarketers are required to check the version of the National Do Not Call Registry that is in effect no more than thirty-one days before making telemarketing calls and may not place calls to consumers' telephone numbers listed on this registry.<sup>138</sup> Fines of up to \$11,000 per violation may be imposed by the FTC against companies that call numbers listed on the National Do Not Call Registry.<sup>139</sup> Mobile phone numbers as well as land-line phone numbers may be registered on the National Do Not Call Registry.<sup>140</sup>

*FTC Prosecution of Telemarketers:* A recent case, *FTC v. Global Marketing Group*, illustrates the FTC's powers to prosecute telemarketers who violate the Telemarketing Sales Rule or § 5's prohibitions on engaging in "deceptive" or "unfair" acts and practices.<sup>141</sup> In this case, the FTC obtained a federal court order to temporarily shut down the company's payment processing operation while it investigated a complaint that the

---

135. 16 C.F.R. § 310.4(d).

136. See generally 16 C.F.R. §§ 310.1-9.

137. See 16 C.F.R. § 310(4)(b)(iii), (iv) (making it a violation of the TSR to make a telemarketing call to a consumer on the National Do Not Call Registry).

138. 16 C.F.R. § 310(4)(b)(iv). Telemarketers pay a fee to access the National Do Not Call Registry. See generally 16 C.F.R. § 310.8. See also FTC, Telemarketing Sales Rules Fees, 16 C.F.R. Part 310, available at <http://www.ftc.gov/os/2006/07/P034305TSRFeesFinalRuleFRNotice.pdf>.

139. *FTC "Do Not Call" Crackdown Nets \$7.7 Million in Fines*, SILICONVALLEY.COM (Nov. 7, 2007) (reporting that federal regulators announced nearly \$7.7 million in settlements with six companies that it investigated for calling people on the national Do Not Call list).

140. See Press Release, FTC, The Truth about Cell Phones and the Do Not Call Registry, (June 21, 2006), available at <http://www.ftc.gov/opa/2006/06/dnccellphones.htm>. The National Do Not Call Registry accepts registrations from both cell phones and land lines. There is currently no directory of wireless phone numbers. The telecommunications industry has been discussing the possibility of creating a wireless 411 directory, and according to the cell phone industry, cell phone numbers will not be listed in a wireless 411 directory unless subscribers want them to be included in the directory, i.e., subscribers will have to "opt-in." *Id.*

141. See generally Complaint for Injunctive and Other Equitable Relief, *FTC v. Global Mktg. Group*, No. 8:06CV2272T-30TGW (M.D. Fla. Dec. 11, 2006) [hereinafter *Global Mktg. Group Complaint*]. See also 15 U.S.C. § 45(a) (2001).

company helped telemarketers defraud consumers of millions of dollars.<sup>142</sup> The case involved claims that telemarketers based in Canada ran “advance-fee credit card schemes,” inducing consumers to allow an electronic debit of several hundred dollars from their bank accounts in exchange for unsecured credit cards that the consumers never received.<sup>143</sup> The defendants in the case, who were located in the U.S., ran a payment processing operation in which they debited funds from the consumers’ bank accounts, deducted their processing fees from the gross proceeds, and then forwarded the balance of the proceeds from the deceptive scheme to the telemarketers.<sup>144</sup> The FTC complaint also alleges that defendants engaged in other deceptive and unfair business practices including “list brokering,” which involved selling lead lists to telemarketers to use in deceptive and abusive telemarketing schemes.<sup>145</sup> The lists included consumers’ personal and financial information, such as names, addresses, and telephone numbers, along with bank account and routing numbers that telemarketers used to contact and defraud consumers.<sup>146</sup> The temporary restraining order obtained by the FTC prohibits defendants from processing payments for the telemarketers and otherwise violating the Telephone Sales Rule or the FTC Act, either directly or indirectly, by assisting anyone who falsely represents to consumers that they will, or are likely to, receive unsecured credit cards.<sup>147</sup>

## 2. The Telephone Consumer Protection Act

The Telephone Consumer Protection Act (“TCPA”) was adopted to address certain telemarketing practices that may invade consumer privacy.<sup>148</sup> In addition to FCC and state government enforcement actions,

---

142. See generally *Ex Parte Temporary Restraining Order With Asset Freeze, Other Equitable Relief, and Order to Show Cause Why a Preliminary Injunction Should Not Issue*, FTC v. Global Mktg. Group, No. 8:06-cv-2272-T-30TGW (M.D. Fla, Dec. 12, 2006) [hereinafter *Global Mktg. Group Temporary Restraining Order*]. See Press Release, FTC, *FTC Stops Payment Processor Who Aided Cross-Border Telemarketing Fraud* (December 20, 2006), available at <http://ftc.gov/opa/2006/12/globalmarketing.htm> (notifying the public that the FTC has obtained a temporary restraining order that includes freezing the defendants’ assets while the FTC investigates the complaint).

143. *Global Mktg. Group Complaint*, *supra* note 141, at ¶¶ 16, 17.

144. *Id.*

145. *Id.* at ¶¶ 26, 27.

146. *Id.* The FTC’s complaint does not indicate whether any mobile phone numbers were provided to telemarketers by the defendants.

147. See *Global Mktg. Group Temporary Restraining Order*, *supra* note 142, at 7-9; Press Release, FTC, *FTC Stops Payment Processor Who Aided Cross-Border Telemarketing Fraud* (December 20, 2006), available at <http://ftc.gov/opa/2006/12/globalmarketing.htm>.

148. Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394 (1991) (codified at 47 U.S.C. § 227 (2007)). See also Rules and Regulations Implementing



the TCPA authorizes consumers to sue violators for the greater of \$500 for each violation or actual damages, with the possibility of recovering treble damages.<sup>149</sup> Among other things, the TCPA requires the FCC to implement regulations to protect the privacy rights of citizens by restricting the use of the telephone network for advertising purposes.<sup>150</sup> The FCC has adopted administrative regulations to protect consumer privacy relative to telephone advertising.<sup>151</sup> Given this Article's focus on regulation of advertising activities in m-commerce, the FCC's heightened restrictions on the making of telephone solicitations and telemarketing calls to wireless telephone numbers merit close examination.<sup>152</sup>

*Telemarketers Obligation to Honor Company-Specific Do Not Call Requests by Phone Subscribers and Restrictions on Calls to Residences:* FCC regulations require telephone solicitors to place residential subscribers on a company-specific do-not-call list if they ask the solicitor to put them on the solicitor's do-not-call lists. It also requires companies to establish procedures for company-specific do-not-call lists and to honor subscribers' requests to be placed on companies' do-not-call lists.<sup>153</sup> These regulations also restrict the hours of the day during which telephone solicitations may be made to subscribers' residences (calls may not be made before 8 a.m. or after 9 p.m.).<sup>154</sup>

---

the Telephone Consumer Protection Act of 1991 and Junk Fax Prevention Act of 2005, *Report and Order and Third Order on Reconsideration*, 21 F.C.C.R. 3787, ¶. 2 (2006).

149. 47 U.S.C. § 227(b)(3); 47 U.S.C. § 227(c)(5).

150. 47 U.S.C. § 227(b)(2), (c).

151. See Rules and Regs. Implementing the Tel. Consumer Prot. Act of 1991, *Rpt. and Order*, 7 F.C.C.R. 8752 (1992); Rules and Regs. Implementing the Tel. Consumer Prot. Act of 1991, *Memorandum Opinion and Order*, 10 F.C.C.R. 12391 (1995); Rules and Regs. Implementing the Tel. Consumer Prot. Act of 1991, *Order on Further Reconsideration*, 12 F.C.C.R. 4609 (1997). See also Jaqualin Friend Peterson, Annotation, *Communications Act of 1934 – Telephone Consumer Protection Act*, 74 AM. JUR. 2D § 14 (2006).

152. The TCPA's delivery restrictions apply to wireless phone numbers including "any telephone number assigned to a paging service, cellular telephone service, specialized mobile radio service, or other radio common carrier service, or any service for which the called party is charged for the call." 47 U.S.C. § 227 (b)(iii). See also 47 C.F.R. § 64.1200(a)(iii). See also 47 C.F.R. § 64.1200(e) (clarifying that the making of telephone solicitations or telemarketing calls to wireless telephone numbers is covered by the delivery restrictions set out in sections (c) and (d) of 47 C.F.R. § 64.1200); See generally Rules and Regs. Implementing the Tel. Consumer Prot. Act of 1991, *Rpt. And Order*, 18 F.C.C.R. 14014 (2003) [hereinafter 2003 TCPA Order].

153. See references and accompanying text at *supra* note 151. However, tax-exempt nonprofit organizations are not required to have a do-not-call list for residential subscribers. 47 C.F.R. § 64.1200(d)(7). FCC regulations also prohibit sending unsolicited advertisements to fax machines without prior express invitation or permission of the recipient. 47 C.F.R. § 64.1200(d).

154. 47 C.F.R. § 64.1200(c)(1).

The 2003 TCPA Order specifically addresses the application of the TCPA to wireless telephone numbers.<sup>155</sup> The rules restricting calls to wireless phones distinguish between live calls and other calls that use automatic telephone dialing systems or prerecorded messages.<sup>156</sup> Generally the rules do not prohibit live telemarketing calls to wireless telephone numbers.<sup>157</sup> However, wireless telephone users may register their wireless telephone numbers on the National Do Not Call Registry to restrict telemarketers from having the right to make live telemarketing calls to their wireless phone numbers.<sup>158</sup> Although consumers' registration of their mobile phone numbers on the National Do Not Call Registry will not prevent a telemarketing call from a company that has an established business relationship with a wireless subscriber, a subscriber who receives such live calls may make a company-specific do-not-call request.<sup>159</sup> Additionally, to the extent that live telemarketing calls to wireless customers are permitted because the customers have not opted out by listing their numbers on the National Do Not Call Registry and/or made company-specific do-not-call requests, telemarketers must comply with rules that require complying with time of day restrictions for calls to residential subscribers and are required to establish procedures for, and to maintain, company-specific do-not-call lists.<sup>160</sup>

*Restrictions on Automated and Prerecorded Telemarketing Calls:* The TCPA's restrictions on the making of automated or prerecorded telemarketing calls depend on whether these calls are made to wireless (mobile) phone numbers or made instead to wireline (land-line) phone numbers.

Phone calls to wireless phone numbers that are *not* live calls are generally prohibited by the TCPA.<sup>161</sup> Specifically, it is unlawful under the TCPA to make *any call* using an automatic telephone dialing system

---

155. 2003 TCPA Order, *supra* note 152, at paras. 150-74. One rationale for more restrictive regulations related to telemarketing calls made to wireless customers is that wireless customers are generally charged for incoming calls. *Id.* at para. 165.

156. *Id.* at para. 165.

157. *Id.* at para. 166.

158. *Id.* See also *Mainstream Mktg. Servs., Inc. v. FTC*, 358 F.3d 1228, 1233 (10th Cir. 2004). In *Mainstream Marketing Services*, the court held that establishment of a National Do Not Call registry allowing individuals to register their phone numbers on a National Do Not Call list and prohibiting most commercial telemarketers from calling the numbers on that list was a valid commercial speech regulation that did not violate the First Amendment, even though this government-established "opt-in" regulation does not provide a similar mechanism to limit charitable or political calls. *Id.* at 1246.

159. 2003 TCPA Order, *supra* note 152, at n.612.

160. See 47 C.F.R. § 64.1200(e) (referencing sections (c) and (d) of this rule). The FCC's 2003 TCPA Order states that "we conclude that these rules apply to calls made to wireless telephone numbers." 2003 TCPA Order, *supra* note 152, at para. 167.

161. 2003 TCPA Order, *supra* note 152, at para. 165.

(autodialed calls) or a prerecorded message to any *wireless* telephone number.<sup>162</sup> There is no exception to this prohibition for sellers who have established business relationships with the consumers called and for the call to be legitimate, the caller must obtain the called party's consent. This prohibition on making autodialed calls or sending prerecorded messages covers both voice calls and text message calls to wireless numbers, including short message service ("SMS") calls made to telephone numbers assigned to a wireless service.<sup>163</sup> The rationale for prohibiting *autodialed and prerecorded* calls to wireless customers, while generally permitting *live* telemarketing calls to wireless phone numbers, is that the former are viewed as a greater nuisance and invasion of privacy than live solicitation calls.<sup>164</sup> Additionally, from a policy perspective, prohibiting live telemarketing calls to wireless phone numbers may unduly restrict telemarketers' ability to contact customers who do not object to receiving such calls and may unduly restrict telemarketers from reaching customers who use their wireless phones as their primary or only phones.<sup>165</sup>

Autodialed telemarketing phone calls made to wireline phone numbers are also prohibited under the TCPA.<sup>166</sup> However, the TCPA contains exceptions to its general prohibition on making autodialed telemarketing calls to wireline phone numbers that cover situations where the seller has an established business relationship with the consumer,<sup>167</sup> or the consumer has given prior express invitation or consent to receive the sender's telemarketing calls.<sup>168</sup> When an autodialed telemarketing message

---

162. See 47 U.S.C. § 227(b)(1)(A)(iii); 47 C.F.R. § 64.1200(a)(1)(iii); 2003 TCPA Order, *supra* note 152, at para. 165. An "automatic telephone dialing system" means equipment with the capacity "(A) to store or produce telephone numbers to be called, using a random or sequential number generator; and, (B) to dial such numbers". 47 U.S.C. § 227(a)(1).

163. 2003 TCPA Order, *supra* note 152, at para. 165.

164. *Id.*

165. *Id.* at para. 166.

166. As in the case of live telemarketing calls to wireless phone numbers, the TCPA permits live telemarketing calls to wireline subscribers as long as the calls comply with the TCPA's form and notice requirements. That is, unless the wireline subscribers have registered on the National Do Not Call Registry or made a company-specific do-not-call request. See generally 47 C.F.R. § 64.1200 (c)-(d).

167. 47 C.F.R. 64.1200(a)(2).

168. 47 U.S.C. § 227(a)(4). The regulations also exclude calls for emergency purposes, calls that are not made for a commercial purpose (i.e., do not include a solicitation), and calls made by tax-exempt organizations (i.e., charitable organizations). 47 C.F.R. § 64.1200(a)(2)(i)-(v). The FTC currently has a nonenforcement policy regarding prohibitions on prerecorded telemarketing calls to wireline numbers, but in 2006 proposed rules that would revoke this non-enforcement policy; however, these rules have not yet been implemented. Federal Trade Commission, Denial of Petition for Proposed Rulemaking; Revised Proposed Rule with Request for Public Comments; Revocation of Non-Enforcement Policy; Proposed Rule, 71 Fed. Reg. 58716 (Oct. 4, 2006). Because the FTC

is permitted to a landline phone number, the form of that call is still regulated: for example, time of day restrictions continue to apply.<sup>169</sup>

#### *D. Mobile Carriers' Obligations to Protect Phone Subscribers' Personal Data*

Federal statutes and FCC rules require telecommunications carriers, including mobile carriers, to protect the privacy of certain types of personal information about subscribers that are defined as Customer Proprietary Network Information ("CPNI").<sup>170</sup> Essentially, federal statutes and rules mandate that telecommunications carriers implement minimal fair information practices with respect to use and disclosure of this type of subscribers' personal information.<sup>171</sup> Exhibit D summarizes the federal regulation of data privacy applicable to mobile carriers, VoIP providers, third-party advertisers, and mobile handset manufacturers to protect mobile phone subscribers' personal data that could be used for commercial advantages to deliver m-advertising. These federal laws are essentially data protection laws that provide minimal protection to consumers as subscribers of telecommunications services. The CPNI data privacy rules

---

has not implemented these rules or changed its non-enforcement policy regarding prerecorded telemarketing calls, the discussion in this section is limited to the regulatory limitations on making automated telemarketing calls.

169. See, e.g., 47 C.F.R. §§ 64.1200(a)(5)-(6) (prohibiting disconnection by the seller of an unanswered call before fifteen seconds or four rings; prohibiting the seller from abandoning more than three percent of all telemarketing calls answered by a live person, measured over a thirty day period).

170. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified in 47 U.S.C. § 151-710 (2007); Telecomm. Carriers' Use of Customer Proprietary Network Info. And Other Customer Info., *Second Rpt. And Order and Further Notice of Proposed RM*, 13 F.C.C.R. 8061 (1998) [hereinafter CPNI Order 1998]. See also Telecomm. Carriers' Use of Customer Proprietary Network Info. And Other Customer Info., *Third Rpt. and Order and Third Further Notice of RM*, 17 F.C.C.R. 14860, paras. 5-25 (2002) (summarizing the history of the CPNI Order, including amendments by the FCC to the original CPNI Order).

171. See Darren Handler, *The Wild, Wild West: A Privacy Showdown on the Radio Frequency Identification (RFID) Systems Technological Frontier*, 32 W. ST. U.L. REV. 199, 218 (2004) (commenting that "Congress passed the Telecommunications Act [in 1996], which directed telecommunications companies to obtain customer approval prior to selling CPNI [customer proprietary network information] to third parties interested in the data for advertising and marketing purposes"). Handler provides a summary of the limits on CPNI data dissemination by telecommunications carriers as these limits existed prior to the 2007 CPNI Order:

The current state of CPNI data dissemination was set forth in 2002 by the Federal Communications Commission (FCC) which allows for both opt-in, prior to release of CPNI to third parties, and for opt-out relating to affiliated party release of CPNI. The FCC Final CPNI Order seems to strike a balance between protecting a customer's right to privacy, concerning transactional data, while not putting too great a strain on the rights of parties interested in disseminating such data.

*Id.* at 219 (internal citations omitted). See also 2007 CPNI Order, *infra* note 174 and accompanying text.

may require businesses to give mobile phone subscribers notice and obtain their consent to use their personal data for m-advertising purposes.

**Exhibit D**

**FCC Regulation of Data Privacy & Mobile Advertising  
Required Consent to Collect, Use, Allow Access or Disclose Subscribers’  
Personal Data**

	<b>Mobile Carrier</b>	<b>VoIP Provider</b>	<b>Third Party M-Advertiser</b>	<b>Mobile Handset Manufacturer</b>
<b>Carrier may collect, use, disclose and permit access to CPNI to provide subscriber services to its customers?</b>	Yes, customer authorization is implied under the total service approach definition of the customer’s existing relationship with the carrier.	Yes, not regulated.	Yes, not regulated, but crime of pretexting may apply.	Yes, not regulated, but crime of pretexting may apply.
<b>Carrier may use CPNI to market communications-related services to its customers? (Other Regulation May Restrict M-Ads: see CANSPAM and the Telemarketing Sales Rule).</b>	Yes, either “opt-in” or “opt-out” customer authorization mechanisms may be used. 2007 CPNI Order does not change this.	2007 CPNI Order brings VoIP providers under CPNI rules.	Yes, not regulated, but the crime of pretexting may apply.	Yes, not regulated, but crime of pretexting may apply.
<b>Access to or disclosure of CPNI may be allowed by Carrier to its affiliates and agents for marketing communications-related services? (location data of inbound or outbound calls; billing data; phone numbers called)</b>	Yes, either “opt-in” or “opt-out” customer authorization mechanisms may be used. The 2007 CPNI Order does not change this.	Yes, 2007 CPNI Order brings VoIP providers under CPNI rules.	Yes, not regulated, but crime of pretexting may apply.	Yes, not regulated, but crime of pretexting may apply.
<b>Access to or disclosure of CPNI allowed by carrier to joint venture partners or independent contractors for marketing purposes (including marketing of communications-related services)</b>	Prior to the 2007 CPNI Order, either “opt-in” or “opt-out” allowed. The 2007 CPNI Order requires “opt-in” consent for disclosures of CPNI to these third parties to enable marketing of communications-related services.	Yes, 2007 CPNI Order requires “opt-in” consent.	Yes, not regulated, but crime of pretexting may apply.	Yes, not regulated, but crime of pretexting may apply.
<b>Subscriber data may be disclosed? Examples: Name, address, phone number (wireline or wireless)</b>	Yes, but disclosures for directory purposes must be non-discriminatory. (Currently carriers do not release official information for wireless	Yes, not regulated.	Yes, not regulated.	Yes, not regulated.

	directories).			
Aggregate data may be disclosed?	Yes, exception to CPNI rules.	Yes, exception to CPNI rules.	Yes, not regulated.	Yes, not regulated.
Exceptions	2007 CPNI Order's "Business Customer Exception" allows alternate privacy protections under agreement with carrier.	2007 CPNI Order's "Business Customer Exception."	N/A, but possible FTC enforcement action for breach of privacy policy, etc.	N/A, but possible FTC enforcement action.

Section 222 of the Telecommunications Act of 1996 ("Telecomm Act") is designed to protect the privacy of telecommunications users with respect to certain types of personal information related to subscription phone service.<sup>172</sup> All telecommunications carriers have a duty to protect the privacy of customers' personal information ("proprietary information") under the Telecomm Act.<sup>173</sup> Three categories of protected customer information are protected by the Telecomm Act: 1) customer proprietary network information ("CPNI") (e.g., the time, date, duration, and destination number of each telephone call made by the subscriber, the type of network that the customer subscribes to, and any other information that appears on the subscriber's telephone bill), 2) aggregate lists of CPNI that do not reveal customers' identities, and 3) subscriber list information (the type of information that would be included in a telephone directory).<sup>174</sup> CPNI is the most sensitive type of customer information; thus, § 222 imposes the highest level of obligations on the carrier with respect to

172. Communications Act of 1934, ch. 652, § 222, 48 Stat. 1064 (codified at 47 U.S.C. § 222 (2001)). The Telecomm Act updated the Communications Act of 1934 to cover new technologies including the Internet, cable, and cellular phones, and included privacy protections for consumers. Edmundson, *supra* note 46, at 219.

173. 47 U.S.C. § 222(a) (providing that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier"). This duty extends to proprietary information of customers that is received from another carrier for purposes of providing any telecommunications service, and the carrier receiving such proprietary information is allowed to use it only for such purposes and not for its own marketing efforts. 47 U.S.C. § 222(b).

174. See Telecomm. Carriers' Use of Customer Proprietary Network Info. And Other Customer Info., *Rpt. And Order and Further Notice of Proposed RM*, 22 F.C.C.R. 6927, para. 4 (2007) [hereinafter 2007 CPNI Order] (discussing the calibration of the protection of personal information under the § 222 framework based on the sensitivity of such information and noting that "Congress accorded CPNI ... the greatest level of protection under this framework"), available at [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/FCC-07-22A1.doc](http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.doc). See Andrew Dymek, Note, *A Clash Between Commercial Speech and Individual Privacy*: U.S. West v. FCC, 2000 Utah L. Rev. 603, 610 (2000) (describing the three types of customer information covered by § 222 of the Telecomm Act).

protecting this type of information.<sup>175</sup> The types of information described in items 2) and 3) above are considered less sensitive, and § 222 imposes fewer limitations on carrier's ability to provide access to or release subscribers' personal information for marketing purposes.<sup>176</sup>

On April 2, 2007, the FCC issued an order designed to strengthen its current privacy rules related to CPNI.<sup>177</sup> The 2007 CPNI Order significantly strengthens consumers' privacy protections including the consumer consent requirements for carriers to use or disclose CPNI. Significantly, the carrier must obtain "opt-in" consent from subscribers before allowing access to or disclosing CPNI to its joint venture partners or independent contractors.<sup>178</sup> Carriers must now obtain advance consent from subscribers before allowing access to or disclosing their personal data to third parties for marketing purposes, including the marketing of communications-related services, as described in more detail in this section. The new "opt-in" consent provisions do not change the previous rules that allowed carriers to use either "opt-in" or "opt-out" subscriber consent mechanisms related to their own marketing of communications-related services to their customers.<sup>179</sup> Further, carriers may also continue to use either "opt-in" or "opt-out" subscriber consent mechanisms to authorize the carrier to provide access to or disclose subscribers' CPNI to their

---

175. See 2007 CPNI Order, *supra* note 174, at para. 4.

176. See 47 U.S.C. § 222(c)(3) (allowing a telecommunications carrier to use, disclose, or permit access to aggregate customer information that is not individually identifiable as long as it provides the aggregate information to other carriers or persons on reasonable nondiscriminatory terms, etc.). Aggregate information is defined as "collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed." 47 U.S.C. § 222(h)(2). See also 47 U.S.C. § 222(c)(1).

177. Press Release, Federal Communications Commission, FCC Strengthens Privacy Rules to Prevent Pretexting, (Apr. 2, 2007) [hereinafter FCC Press Release (Apr. 2, 2007)] available at [http://fjallfoss.fcc.gov/edocs\\_public/attachmatch/DOC-272008A1.pdf](http://fjallfoss.fcc.gov/edocs_public/attachmatch/DOC-272008A1.pdf). See also 2007 CPNI Order, *supra* note 174, at App. B. This appendix contains Final Rules that amend Subpart U of Part 64 of Title 47 of the Code of Federal Regulations with respect to Customer Proprietary Network Information. *Id.* at App. B. In the 2007 CPNI Order, the FCC also seeks comments on whether it should further modify its rules to provide additional privacy protections for consumers. *Id.* at para. 67 (seeking comments on the need to expand consumer protections to ensure that customer information and CPNI are protected in the context of mobile communication devices). See Further Notice of Proposed RM: Customer Proprietary Network Info., *Comments of Consumer Action et al.*, CC Dkt. No. 96-115 (July 9, 2007), available at [http://www.epic.org/privacy/cpni/cpni\\_070607.pdf](http://www.epic.org/privacy/cpni/cpni_070607.pdf).

178. 2007 CPNI Order, *supra* note 174, at 22-23 (discussing the modification of the FCC rules to require telecommunications carriers to obtain "opt-in" consent in the form of express prior authorization from a customer before disclosing that customer's CPNI to a carrier's joint venture partner or independent contractor for the purpose of marketing communications-related services to that customer).

179. 2007 CPNI Order, *supra* note 174, at App. B, Subpart U, 4(b) (amending 47 C.F.R. § 64.2007).

*affiliates and agents* that provide communications-related services so that these entities may use subscribers' personal data to market these services to subscribers.<sup>180</sup>

Additionally, the 2007 CPNI Order clarifies that VoIP and other IP-enabled Internet telephony service providers must also comply with the CPNI rules.<sup>181</sup> Previously it was not clear whether VoIP and other Internet telephony service providers were subject to less rigorous regulation by the FCC as providers of "information services," as compared to telecommunications carriers, who are generally more heavily regulated by the FCC.<sup>182</sup> The 2007 CPNI Order is now in effect.<sup>183</sup> Under this Order, subscribers of VoIP services are entitled to the same consumer privacy protections for CPNI that are available to consumers who subscribe from regular telecommunications carriers.<sup>184</sup>

---

180. *Id.* ("We note that this minor modification to our rules does not affect the opt-out regime for intra-company use of CPNI beyond the total service approach, or the disclosure of CPNI to a carrier's agents or affiliates that provide communications-related services.")

181. 2007 CPNI Order, *supra* note 174, at paras. 54-59. See also Sunny Lu, *Cellco Partnership v. FCC & Vonage Holdings Corp. v. Minnesota Public Utilities Commission: VoIP's Shifting Legal and Political Landscape*, 20 BERKELEY TECH. L.J. 859 (2005). According to Lu:

VoIP is a communication technology in which the analog audio signals of communication are turned into digital data that can be transmitted over the Internet. Instead of the circuit switching of traditional telephony, VoIP features "packet switching," wherein telephone calls are broken into bits of data using the Internet Protocol (IP), and then delivered over the Internet. IP is the most common method for electronic devices to communicate. VoIP providers offer consumers one or more choices among three general ways to communicate: computer-to-computer, telephone-to-computer (and vice-versa), and telephone-to-telephone.

*Id.* at 863.

182. See generally RAYMOND T. NIMMER, LAW OF COMPUTER TECHNOLOGY §16:41 (2006) (discussing the distinction in federal communications law between telecommunications services and information services). For regulatory purposes, the FCC classifies VoIP services according to the network on which the call originates and ends. See also Lu, *supra* note 181, at 864 (reporting that the FCC ruled in February 2004 that VoIP providers were exempt from regulations because calls made in computer-to-computer VoIP never utilize the public switched telephone network (PSTN)). Likewise computer-to-telephone VoIP calls originate on the PSTN and end on the Internet (or vice versa); the FCC has ruled that these types of services are preempted from state regulation and has "hinted" that such services are *information services* that are exempt from most of the traditional federal telephony regulations. *Id.*

183. Cheryl A. Tritt, *Telecommunications Future*, in 25<sup>th</sup> Annual Institute on Telecommunications Policy & Regulation, Practising Law Institute 171 (2007) (stating that the effective date of the 2007 CPNI Order was December 8, 2007). See *infra* notes 211-212 for analysis of the 2007 CPNI Order including its effective date and discussion of First Amendment challenge by regulated industry to the new "opt-in" rule for disclosures of CPNI to joint venture partners and independent contractors.

184. 2007 CPNI Order, *supra* note 174, at para. 61 (discussing the timeline for implementation). Congressional action to require VoIP providers to comply with the CPNI rules had been initiated at the time that the 2007 CPNI Order was issued. See also Prevention of Fraudulent Access to Phone Records Act, 110th Cong. §§ 104(2),



Of particular importance to m-advertising is (a) whether the Telecom Act restricts access by marketers to individual callers' mobile phone numbers, and (b) what level of privacy protection the Act provides for information about the mobile phone users' geographic locations ("location information"). As discussed below, location information is regulated as CPNI, while access to mobile phone numbers is regulated as subscriber list information.

### 1. Customer Proprietary Network Information.

Section 222(c) of the Telecomm Act protects consumers' information privacy by requiring the telecommunication carrier to obtain customer approval before using, disclosing, or permitting access to specific types of personal information that fall within the definition of CPNI, as follows:

Except as required by law or with the *approval of the customer*, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.<sup>185</sup>

Exceptions permit telecommunications carriers to use, disclose, or permit access to customers' CPNI without customer approval in order to conduct billing for telecommunications services, to protect the rights or property of the carrier, and to protect users from fraudulent use of telecommunications services.<sup>186</sup> Additionally, a telecommunications carrier may use, disclose, or permit access to a customer's CPNI without customer approval if it receives an inbound telemarketing call to a "customer for the duration of the call, if such call was initiated by the customer and the customer approves of the use of such information to provide such service."<sup>187</sup> Finally, the carrier does not need to obtain customer approval to provide location information for emergency response purposes or to inform the user's legal

---

203(h)(A)(vii) (Feb. 8, 2007) (extending the privacy obligations of telecommunications carriers under of 47 U.S.C. § 222 to include providers of "real-time Internet protocol-enabled voice communication," thus requiring VoIP telephone service providers to protect the CPNI of their customers) [hereinafter H.R. 936].

185. 47 U.S.C. § 222(c)(1) (emphasis added). Section 222(c)(2) requires a telecommunications carrier to disclose customer proprietary network information upon the affirmative written request by the customer, to any person designated by the customer. 47 U.S.C. § 222(c)(2).

186. 47 U.S.C. § 222(d)(1)-(2).

187. 47 U.S.C. § 222(d)(3).

guardian or user's immediate family in an emergency situation that involves risk of death or serious physical harm.<sup>188</sup>

*The Scope of CPNI:* Only certain types of personal information about customers are within the scope of CPNI. CPNI is defined as:

(A) 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, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and

(B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information.<sup>189</sup>

*Location Data is CPNI:* The Telecomm Act was amended by the Wireless Communications Public Safety Act of 1999 to include "location" in the definition of CPNI.<sup>190</sup> The 2007 CPNI Order revised the CPNI regulations to include a definition of "call detail information" that encompasses information about the transmission of specific telephone calls and expressly includes the location from which an inbound or outbound call was made.<sup>191</sup> As call detail information is a component of CPNI, location information for mobile phone users is protected as CPNI.<sup>192</sup>

*"Opt-in" Customer Consent is Required to Disclose Location Data:* Amendments to the Telecomm Act by the Wireless Communications Public Safety Act of 1999 also specifically addressed wireless location information and the required customer consent for use, disclosure, or providing access to location information as follows: "[W]ithout the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to . . . call location information concerning the user of a commercial mobile service . . ." <sup>193</sup>

The difference in wording between "approval of the customer" required in § 222(c) and "express prior authorization" required by the Wireless Communications Public Safety Act creates uncertainty about the type of consent that a telecommunications carrier must obtain from a

---

188. 47 U.S.C. § 222(d)(4).

189. 47 U.S.C. § 222(h)(1).

190. Wireless Communications and Public Safety Act of 1999, 47 U.S.C. § 609 (1999).

191. 2007 CPNI Order, *supra* note 174, at App. B, Subpart U, 2(d). Call detail information is: "Any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, *location*, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, *location*, or duration of any call." *Id.* (emphasis added).

192. *Id.*

193. 47 U.S.C. § 222(f) (emphasis added). There is an exception to this rule that allows release of customer location information in emergencies. 47 U.S.C. § 222(d)(4).

customer in order to use or release location data and other CPNI about a wireless customer.<sup>194</sup>

*“Opt-in” Consent is Required to Disclose CPNI to the Carrier’s Joint Venture Partners and Independent Contractors for Marketing Purposes:* Rulemaking by the FCC and a federal court decision have helped clarify the meaning of § 222(c)’s requirement that carriers obtain “approval of the customer” to disclose CPNI to their affiliates and third parties for marketing purposes.<sup>195</sup> Initially, the FCC issued an order adopting an “opt-in” approach<sup>196</sup> that required telecommunications carriers to obtain prior express approval before releasing customers’ CPNI to companies for purposes outside the customers’ existing relationship with the carrier.<sup>197</sup> U.S. West challenged the order, arguing that an “opt-out” approach, rather than an “opt-in” approach, should have been specified in the FCC’s order to allow the carrier to infer approval from customers to use, access, or release their CPNI unless customers specifically requested that the carrier limit further use of their CPNI.<sup>198</sup>

In *U.S. West v. FCC*, the Tenth Circuit Court of Appeals struck down the FCC’s “opt-in” requirement as a violation of commercial free speech under the U.S. Constitution.<sup>199</sup> The FCC responded by issuing another order that adopted an “opt-out” standard for § 222 to the extent that it involved intracompany uses of CPNI.<sup>200</sup> Intracompany uses were specified to include the “sharing of CPNI with, and use by, a carrier’s joint venture partners and independent contractors in connection with communications-related services that are provided by the carrier (or its affiliates) individually, or together with the joint venture partner.”<sup>201</sup> “Communications-related services” is a term defined by administrative

---

194. Edmundson, *supra* note 46, at 220-21.

195. The term “affiliate” is defined by the Communications Act of 1934. 47 U.S.C. § 153(1); 47 C.F.R. § 64.2003(a). An affiliate “means a person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another person . . . the term ‘own’ means to own an equity interest (or the equivalent thereof) of more than 10 percent.”

196. Administrative regulations define “opt-in approval” as a “method for obtaining customer consent to use, disclose, or permit access to the customer’s CPNI” that requires that the carrier “obtain from the customer affirmative, express consent allowing the requested CPNI usage, disclosure, or access” after the customer has been provided appropriate notification of the carrier’s request. 47 C.F.R. § 64.2003(h). *See generally* 47 C.F.R. § 64.2008 (specifying the notice required for use of customer proprietary network information).

197. CPNI Order 1998, *supra* note 170, at para. 4.

198. *U.S. West v. FCC*, 182 F.3d 1224 (10th Cir. 1999).

199. *Id.* at 1240.

200. *See* Implementation of the Telecomm. Act of 1996, *Third Rpt. and Order*, 17 F.C.C.R. 14860 ¶. 31 (2002) [hereinafter CPNI Order 2002].

201. *Id.* at ¶ 32.

regulations to mean “telecommunications services, information services typically provided by telecommunications carriers, and services related to the provision or maintenance of customer premises equipment.”<sup>202</sup> Information services typically provided by telecommunications carriers includes Internet access or voice mail services but does not include retail consumer services provided using Internet Web sites, such as travel reservation services or mortgage lending services.<sup>203</sup>

Despite the Tenth Circuit’s decision in *U.S. West*, the FCC retained the “opt-in” consent standard for other disclosures of customers’ CPNI such as disclosures to third parties and affiliates of the carrier who provide no communications-related services.<sup>204</sup> Apparently, the FCC did not view requiring “opt-in” consent for disclosures of CPNI by carriers to third parties and affiliates who provide no communications-related services to be inconsistent with the *U.S. West* case, and no subsequent court opinion resolved the question of when requiring “opt-in” consent violates commercial free speech rights.<sup>205</sup>

The 2007 CPNI Order has changed this and now requires the subscriber to give “opt-in” consent before CPNI access and disclosures may be afforded to the carrier’s joint venture partners and independent contractors (but not for access or disclosures to affiliates and agents of the carrier that provide communications-related services).<sup>206</sup>

Carriers must now obtain “opt-in” consent from subscribers before allowing access or disclosing subscribers’ CPNI to the carriers’ joint venture partners or independent contractors, even to market communications-related services to subscribers.<sup>207</sup> Disclosure of CPNI to affiliates and other third parties for purposes that are not related to

202. 47 C.F.R. § 64.2003(b) (2006).

203. *See* 47 C.F.R. § 64.2003(f) (2006).

204. *See* CPNI Order 2002, *supra* note 200, at ¶¶ 50-51, 56 (“[S]ection 222 and the Commission’s rules concerning use of CPNI are not applicable to those unknown third parties that receive the customer’s personal information . . . . [T]here is a greater need to ensure express consent from an approval mechanism for third party disclosure. Opt-in directly and materially advances this interest by mandating that carriers provide prior notice to customers and refrain from disclosing CPNI unless a customer gives her express consent by written, oral, or electronic means.”).

205. *Id.* According to the 2007 CPNI Order: “Except as required by law, carriers may not disclose CPNI to third parties, or to their own affiliates that do not provide communications-related services, unless the consumer has given opt-in consent, which is express written, oral, or electronic consent.” 47 C.F.R. §§ 64.2005(b), 64.2007(b)(3), 64.2008(e); *see also* 47 C.F.R. § 64.2003(h) (defining “opt-in approval”).

206. *See* 2007 CPNI Order, *supra* note 174 at app. B, para. 4 (amending 47 C.F.R. § 64.2007).

207. *Id.* at 40 (providing that “The Order shall become effective upon publication in the Federal Register subject to OMB approval for new information collection requirements or six months after the Order’s effective date, whichever is later”).

marketing communications services continues to require “opt-in” consent from subscribers.<sup>208</sup>

In its order announcing the new CPNI rules, the FCC discusses *U.S. West* and subsequent court cases that have addressed the regulation of commercial speech.<sup>209</sup> The FCC’s Order provides the agency’s rationale for concluding that requiring an “opt-in” approach for disclosures of CPNI to the carriers’ joint venture partners and independent contractors to market communications related services and to any third parties for general marketing purposes does not violate the carriers’ constitutional commercial free speech rights.<sup>210</sup>

Recently, the National Cable and Telecommunications Association (“NCTA”) filed a complaint with a federal appeals court challenging the new CPNI rules.<sup>211</sup> The NCTA’s petition for review asks the U.S. Court of Appeals to vacate the 2007 CPNI Order’s “opt-in” rule for disclosure of CPNI to its members’ joint venture partners and independent contractors on the basis that the rule violates NCTA members’ constitutional free speech rights under the First Amendment and because it is arbitrary and capricious.<sup>212</sup>

## 2. Subscriber List Information and Access to Mobile Phone Numbers

The Telecomm Act requires telecommunications carriers who provide telephone exchange services to provide subscriber list information gathered in their capacity as providers of such services on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions, to any person upon request for the purpose of publishing directories in any

---

208. *See id.* at ¶. 37.

209. *Id.* at para. 44, n.138 (citing *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n.*, 447 U.S. 557, 564-65 (1980), which provides “that if the commercial speech concerns lawful activity and is not misleading, the government may restrict the speech only if it (1) ‘has a substantial state interest in regulating the speech, (2) the regulation directly and materially advances that interest, and (3) the regulation is no more extensive than necessary to serve the interest.’”).

210. 2007 CPNI Order, *supra* note 174, at ¶ 45.

211. *National Cable and Telecommunications Ass’n v. FCC*, Petition for Review, Case No. 07-1312, U.S. Court of Appeals (D.C. Cir., Aug. 7, 2007) (appealing the CPNI Order, focusing on the “opt in” rule for sharing of CPNI by members with members’ joint venture partners and independent contractors) [hereinafter *NCTA v. FCC*], available at <http://www.ncta.com/DocumentBinary.aspx?id=625>; *see also*, CPNI, Electronic Privacy Information Center, available at <http://www.epic.org/privacy/cpni/>.

212. *Quest Communications International, Inc.* has been permitted to intervene as a respondent in the Case. Order, *NTCA v. FCC*, U.S. Court of Appeals, D.C. Circuit (Sept. 19, 2007). Briefing in the case is scheduled to be completed by June 4, 2008. Order, U.S. Court of Appeals, D.C. Circuit (Jan. 24, 2008).

format.<sup>213</sup> Subscriber list information includes subscribers' names, telephone numbers, and addresses.<sup>214</sup>

The term "subscriber list information" means any information – (A) identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and (B) that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format.<sup>215</sup>

The category of "subscriber list information" is important for this discussion of m-advertising because the telecommunications carrier must provide the statutorily required access to subscriber list information for directory publishing purposes and need not obtain the approval of its customers who would be required to use, release, or permit access to CPNI.<sup>216</sup> Although subscribers' telephone numbers are expressly included in the definition of subscriber list information, the Telecomm Act does not specify whether mobile phone numbers should receive any additional privacy protection as compared to wireline phone numbers.<sup>217</sup>

Currently, telecommunications carriers in the U.S. do not release directories of consumers' wireless telephone numbers.<sup>218</sup> The telecommunications industry has been discussing the possibility of creating a wireless 411 directory.<sup>219</sup> Proposed legislation introduced in the House of Representatives in 2007 would prohibit telecommunications carriers from disclosing a customer's wireless phone number or permitting access to a customer's wireless phone number except with "prior express authorization from the customer."<sup>220</sup>

However, even if Congress does not adopt legislation that would require carriers or other businesses to obtain prior express consent before publishing a directory of wireless phone numbers or permitting third party access to customers' wireless phone numbers, most telemarketing calls to cell phones would still be illegal, and this is true even if the calls are made to wireless phone numbers that are not listed on the National Do Not Call

---

213. See 47 U.S.C. § 222(e) (2000) (specifying that the obligation by telecommunication carriers to provide subscriber information is notwithstanding the telecommunication carriers' obligations under 47 U.S.C. 222(b), (c), and (d)).

214. See Nimmer, *supra* note 182, at § 16:41.

215. 47 U.S.C. § 222(h)(3) (2000).

216. 47 U.S.C. § 222(c)(1) (2000); see Dymek, *supra* note 174, at 611.

217. 47 U.S.C. § 222(c)(1).

218. Press Release, FTC, *supra* note 140.

219. *Id.*

220. H.R. 936, *supra* note 184, at § 202(a)(1)(E).

Registry.<sup>221</sup> This is because telemarketers generally use automated dialing equipment to make telemarketing phone calls and current FCC regulations prohibit telemarketers from using automated dialers when calling cell phone numbers unless the caller has the prior express consent of the called party.<sup>222</sup>

Some cellular phone companies have used the civil litigation process to recover judgments from companies that have wrongfully collected private cell phone numbers and other proprietary data about their customers. For example, Cingular Wireless sued 1st Source, a data mining company, and recovered a judgment of over \$1.1 million from the company for using fraud, computer hacking, and “social engineering” to collect the private cell phone numbers and calling histories of its customers.<sup>223</sup> In the lawsuit, Cingular claimed that 1st Source obtained customers’ confidential proprietary data by tricking Cingular’s customer representatives into releasing the data or gaining unauthorized access to online account information that was stored on Cingular’s database.<sup>224</sup>

### 3. Federal Preemption Limits State Law Regulation of Telecommunications Carriers That Aim to Enhance Telephone Subscribers’ Personal Data Protection

Federal preemption of state law has been found with respect to CPNI and network disclosure rules.<sup>225</sup> Federal preemption occurs when Congress, by legislation, exercises its paramount authority over a subject such that it suspends the power of the states to regulate on a topic, such as the transmission of interstate messages and the facilities for such transmission.<sup>226</sup> Given the extensive federal regulation of personal data related to customers’ CPNI and the interstate nature of mobile phone transactions, it is likely that regulations by states attempting to require telecommunications carriers to provide additional privacy protections for

---

221. Press Release, FTC, *supra* note 140 (attributing this conclusion to the FCC).

222. See *supra* Section V.C.2. for a discussion of FCC regulation of telemarketing calls to cell phones.

223. See Greg Land, *Cingular Wins \$1.1M Victory Over Data Miners*, LAW.COM (Nov. 29, 2006), <http://www.law.com/jsp/article.jsp?id=1164636901736>.

224. See *id.*

225. 74 AM. JUR. 2D *Telecommunications* § 18 (2001) (citing *People v. California*, 39 F.3d 919 (9th Cir. 1994) and *Southwest Bell Tel. Co. v. Pub. Util. Comm’n*, 812 F. Supp. 706 (W.D. Tex. 1993)).

226. See *id.* See also Dymek, *supra* note 174, at 610 n.41 (“The 1996 Telecommunications Act expressly preempts any state laws that prohibit or have the effect of prohibiting the ability of any entity to provide any interstate or intrastate telecommunications service.”) (internal quotation and citation omitted).

mobile customers with respect to their mobile phone services would be preempted and thus invalid.<sup>227</sup>

#### 4. Legislative and Administrative Proposals Aim to Enhance Consumer Privacy Protections for Telephone Records and Mobile Phone Numbers

In 2006, the FCC issued a Notice of Proposed Rulemaking (“Notice”) seeking comments on what steps, if any, it should take to further protect CPNI from unauthorized access by third parties.<sup>228</sup> The Notice followed the filing of a petition by the Electronic Privacy Information Center (“EPIC”) claiming that CPNI is not adequately protected under the FCC’s current rules and pointing out that numerous Web sites advertise the sale of personal telephone records obtained without the caller’s knowledge or consent.<sup>229</sup> The FCC’s Notice sought comment on additional steps that it could take to adequately protect CPNI, including five security measures proposed by EPIC.<sup>230</sup> As discussed previously, the FCC has since adopted final rules that enhance CPNI protection, although these new regulations do not protect the privacy of consumers’ cell phone numbers.<sup>231</sup>

Additionally, legislation has been introduced in Congress to provide additional protections for consumer privacy that would require telecommunications carriers to provide customers with specific privacy protections for wireless phone numbers and subscribers’ geographic location information.<sup>232</sup> For example, a bill was introduced in the House of Representatives that would restrict telecommunications carriers from permitting access to or disclosing the wireless telephone number of any

---

227. However, *see infra* Section V.E. for a discussion of the new federal criminal law related to pretexting, which expressly permits states to provide additional protections for consumers with respect to pretexting activities. The preservation of state authority to pass laws that punish pretexting more harshly than the federal law is likely due to the fact that pretexting is a type of fraud committed by third parties and such state laws do not attempt to regulate the privacy practices of telecommunications carriers.

228. *See* Clare Liedquist, *Selected FCC Docket Summaries, 2005-2006, Implementation of the Telecomms. Act of 1996, Notice of Proposed Rulemaking*, 21 *F.C.C.R.* 1782 (Feb. 10, 2006), 14 *COMM.LAW CONSPLECTUS* 599, 599 (2006).

229. *Id.*

230. *See id.* at 599-600 (listing the five security measures suggested by EPIC: “(1) using consumer-set passwords (as opposed to common biographical data that are readily available through public records); (2) maintaining a record of all instances when a customer’s records have been accessed; (3) encrypting all personal records; (4) limiting data retention; and (5) notifying customers when their CPNI may have been improperly disclosed.”).

231. *See supra* notes 177-183, 213-217.

232. *See* Wireless Privacy Protection Act of 2005, H.R. 83, 109th Cong. (2005) (introduced Jan. 4, 2005 to amend § 222 of the Communications Act of 1934 to require customer consent to the provision of wireless call location information).



customer.<sup>233</sup> Wireless telephone numbers and/or location information are commercially useful data for m-advertisers, so passage of this type of legislation may restrict the growth of m-advertising applications, especially if advertisers are required by law to obtain prior express authorization from mobile phone subscribers to include their mobile phone numbers on m-advertising lists or to generate location-specific m-advertising. This legislation has not yet been passed in the House of Representatives or the Senate.

### *E. Obtaining Subscribers' Phone Records by "Pretexting" Is a Federal Crime*

The problem of phone record pretexting gained national attention in 2006 when it became public that Hewlett Packard Company ("HP") had hired investigators to look into boardroom leaks and that those investigators had used pretexting to obtain phone records of HP board members and journalists.<sup>234</sup> At the time of HP's actions, pretexting to obtain phone records was not a federal crime, although it was against the law in some states like California.<sup>235</sup> HP agreed to pay \$14.5 million to settle a civil lawsuit brought by the State of California's Attorney General that accused the company of unfair business practices related to its use of pretexting to investigate the board leak.<sup>236</sup>

In 2006, Congress passed the Telephone Records and Privacy Protection Act.<sup>237</sup> The new law criminalizes "pretexting," which generally involves pretending to be someone else in order to access confidential phone records of the other person from telecommunications carriers or providers of IP-enabled voice service (Internet phone companies).<sup>238</sup> Confidential phone records covered by the new pretexting law include call log information, such as the phone numbers of persons called by

---

233. See H.R. 936, *supra* note 184, at § 202(a)(1)(E).

234. See Anne Broache, *Senate May Vote on Pretexting Bill This Week*, CNET NEWS.COM (Dec. 8, 2006), [http://www.news.com/Senate-may-vote-on-pretexting-bill-this-week/2100-1028\\_3-6141754.html](http://www.news.com/Senate-may-vote-on-pretexting-bill-this-week/2100-1028_3-6141754.html).

235. *Id.* See also Ryan Blitstein, *CNet Reporters to Sue HP over Pretexting*, SILICONVALLEY.COM (May 7, 2007) (reporting that three CNet reporters are preparing a lawsuit alleging invasion of privacy by HP that is related to HP's access to the journalists' private phone records), [http://www.sccba.com/lawpractice/view\\_newsitem.cfm?id=7929](http://www.sccba.com/lawpractice/view_newsitem.cfm?id=7929).

236. Jordan Robertson, *Suit Over Probe of HP Leaks Settled*, SAN DIEGO UNION-TRIB., Dec. 8, 2006, available at [http://www.signonsandiego.com/uniontrib/20061208/news\\_1b8hp.html](http://www.signonsandiego.com/uniontrib/20061208/news_1b8hp.html); see also Press Release, California Department of Justice, Attorney General Lockyer Announces \$14.5 Million Settlement to Resolve Civil Complaint Related to Pretexting Incident, Dec. 7, 2006, available at <http://ag.ca.gov/newsalerts/release.php?id=1394&year=2006&month=12>.

237. Telephone Records and Privacy Protection Act of 2006, 18 U.S.C. § 1039 (2007).

238. See 18 U.S.C.A. § 1039(a)-(c) (West Supp. 2007); see also 18 U.S.C.A. § 1039(h)(2) (West Supp. 2007).

consumers, which may reveal sensitive information, like the names of the subscribers' doctors, public and private relationships, business associates, etc.<sup>239</sup> The scope of confidential phone records appears broad enough to cover geographic location information about mobile phone users—information that would be useful to m-advertisers for targeting consumers with advertising based on their geographic locations at particular times.

It is now a federal crime punishable by up to ten years in prison to use pretexting to access customers' confidential phone records, including access to wireless and VoIP calling records.<sup>240</sup> Prohibited pretexting behaviors include making false and fraudulent representations, using false documents, or fraudulently accessing online records.<sup>241</sup> The bill also prohibits data brokers from selling phone records that have been obtained by pretext,<sup>242</sup> and penalizes individuals who have received or purchased such records.<sup>243</sup>

However, the new federal statute criminalizing pretexting does not impose additional privacy regulations on telephone carriers or Internet phone service providers, although it prohibits telephone carrier employees from selling customers' confidential phone record information to unauthorized data brokers.<sup>244</sup> The 2007 CPNI Order complements the new federal pretexting statute by requiring carriers (defined for this purpose to include VoIP service providers) to implement new security and privacy protections for subscribers' CPNI that will also help to prevent pretexting.<sup>245</sup>

#### *F. Federal Statutes Protect Mobile Phone Users' Communications from Unlawful Interception or Unauthorized Access*

The Electronic Communications Privacy Act of 1986 ("ECPA") protects the privacy of peoples' wire, oral, and electronic communications from unlawful wiretapping, eavesdropping, and other forms of unauthorized access and disclosure by private businesses, law enforcement,

---

239. See 18 U.S.C.A. § 1039(h) (West Supp. 2007); see also H.R. 4709, 109th Cong. § 2 (2006) (enacted) (explaining the policy concerns this law is designed to address including potential criminal uses of customers' confidential phone data).

240. 18 U.S.C.A. § 1039(a)-(c) (West Supp. 2007). This law exempts law enforcement and does not preempt state laws, so states can still impose tougher penalties to stop pretexting, including tougher penalties on phone record sales.

241. *Id.*

242. *Id.* at § 1039(b).

243. *Id.* at § 1039(c).

244. *Id.* at § 1039(b).

245. See Marguerite Reardon, *FCC Imposes Rules Designed to Prevent Pretexting*, CNET NEWS.COM, Apr. 3, 2007, [http://www.news.com/FCC-imposes-rules-designed-to-prevent-pretexting/2100-1037\\_3-6172705.html](http://www.news.com/FCC-imposes-rules-designed-to-prevent-pretexting/2100-1037_3-6172705.html); see also FCC Press Release, Apr. 2, 2007, *supra* note 177.

and other government officials.<sup>246</sup> The ECPA prohibits *any person*, including businesses and law enforcement, from unlawfully and intentionally intercepting the contents of telephone and other electronic communications or gaining unauthorized access to the contents of electronic communications in electronic storage.<sup>247</sup> Live telephone communications, voice mail messages, email messages, text messages, and instant messages are all forms of wire and electronic communications that are protected by the ECPA. Unless the interception or unauthorized access of a wire, oral, or electronic communication is covered by one of several statutory exceptions or defenses, violation of the ECPA is both a civil violation and a federal crime.<sup>248</sup> However, court decisions interpreting the scope of the ECPA have narrowed its privacy protections, and they effectively provide greater latitude for businesses to monitor wire, oral, and electronic communication systems without violating the ECPA. For example, appellate court decisions have limited the scope of Title I to interceptions of wire, oral, and electronic communications that occur in transit. Specifically, courts have held that the reading of another's email that has been received by the computer server of the intended recipient but not yet read is at most a Title II violation because no interception in transit has occurred.<sup>249</sup> And further, some courts have also limited the scope of Title II by excluding conduct involving the reading of email that has already been read by the intended recipient.<sup>250</sup>

---

246. 18 U.S.C. § 2510 (2000). Although the ECPA's application to government's and law enforcement's interception or access to mobile phone communications is beyond the scope of this Article, government may track cell phones, in real time, without a search warrant under the ECPA by analyzing information as to antennae being contacted by cell phones, so long as tracking does not involve cell phones being used in private places where visual surveillance would not be available. Application of U.S. for an Order Authorizing Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers (Sealed), 402 F. Supp. 2d 597, 604 (D. Md. 2005).

247. See The Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522 [hereinafter Title I], 2701-2712 [hereinafter Title II], 3117, 3121-3127 [hereinafter Pen Register and Trap and Trace Devices].

248. Violators may face fines of up to \$10,000 and imprisonment of up to five years for a Title I violation. 18 U.S.C. §§ 2511(4)(a), 2520(c)(2)(B). Violators may face fines of a minimum of \$1000 per violation and up to ten years in prison for a Title II violation. 18 U.S.C. §§ 2701(b)(1), 2707(c). Citizens may sue for civil damages, punitive damages (if the violation is willful or intentional), attorneys' fees and litigation costs. See 18 U.S.C. §§ 2520(b), 2707(b).

249. *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 876-79 (9th Cir. 2002) (discussing *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457 (5th Cir. 1994), which held that seizure of a computer containing unread email messages was not an unlawful interception of electronic communications because it occurred sometime after the transmission of the email messages to the computer).

250. See *Fraser v. Nationwide Mutual Insurance Co.*, 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001) (holding that the email a company retrieved from its storage site was in "post-transmission storage," having already been sent by the employee and received by the

Beyond these restrictive judicial interpretations of the scope of the ECPA, it is clear that the act only restricts interception or unauthorized access to the *contents* of wire, oral, or electronic communications, and thus is not a broad data protection law, although the distinction between protected contents and other information that is not protected is not always obvious. The general rule is that the ECPA does not restrict access to information about phone conversations, email, or Internet communications that is analogous to the *addressing information* on the outside of a letter sent through the U.S. mail.<sup>251</sup> But is the subject line of an email content or envelope information? One could argue that the subject line of an email is more than mere addressing information because it may include information about the substantive content of the email message. Is an Internet search query content or addressing information? The First Circuit Court of Appeals in the *In re Pharmatrak, Inc. Privacy Litigation*, the Federal Circuit Court of Appeals held that interception of Internet search queries is covered by the ECPA.<sup>252</sup> For example, an Internet search query containing the key words “breast cancer” may reveal sensitive information about the person conducting the Internet search, particularly if it is captured along with PII about the sender of the query, like the sender’s name. Fortunately for the defendant, Pharmatrak, the case was remanded to the district court to determine whether Pharmatrak intended to intercept the contents of electronic communications, a necessary element of an ECPA violation.<sup>253</sup> The district court found that there was no evidence that Pharmatrak intentionally intercepted the electronic communications, and therefore it dismissed the case.<sup>254</sup> Since mobile phones increasingly offer Internet access services, the ECPA and judicial interpretations like those in *Pharmatrak* will likely be applied to restrict interception or unauthorized access by third party advertisers to the contents of subscribers’ mobile Internet searches. The ECPA will also protect the privacy of other sorts of mobile communications such as the contents of text messages, voice-mail messages, and live mobile phone conversations.

There are broad statutory exceptions to the scope of Title I and Title II of the ECPA, which exempt an array of interceptions and unauthorized

---

intended recipient, so was not covered by Title II); *but see* Theofel v. Farey-Jones, 359 F.3d 1066, 1075-77 (9th Cir. 2004) (finding *Fraser’s* interpretation of Title II to be flawed and that “prior access is irrelevant to whether the messages at issue were in electronic storage”).

251. *See* SOLOVE ET AL., *supra* note 29, at 283-84 (quoting Orin Kerr’s explanation of the distinction between content and envelope information but arguing that the distinction breaks down when applied to IP addresses and URLs, and questioning the wisdom of offering lower privacy protection for noncontent information).

252. *See* *Pharmatrak, Inc. Privacy Litigation*, 329 F.3d 9, 13 (1st Cir. 2003).

253. *Id.*

254. *See* *Pharmatrak, Inc. Privacy Litigation*, 292 F. Supp. 2d 263, 268 (D. Mass. 2003).

access situations from its privacy protections. These statutory exceptions will have the effect of significantly reducing the privacy expectations of mobile phone users with respect to their mobile phone conversations and m-commerce transactions. For example, two statutory exceptions in Title I exclude from its coverage interceptions by “providers of communications systems,” (“provider exception”)<sup>255</sup> and interceptions with “consent” (“consent exception”).<sup>256</sup> The Title I exemption for interceptions by providers does not authorize the provider to monitor purely personal communications, however. In the workplace context, courts have found interception of employees’ personal phone calls on business premises are not exempt under Title I when the interception continues after the intercepting business is aware of the personal nature of the call.<sup>257</sup> Title II also embraces the provider and consent exceptions.<sup>258</sup> In the workplace context, employer interceptions or access to employees’ private phone and electronic communications have been found to violate the ECPA when not protected by one of these exceptions.<sup>259</sup>

The scope of the provider exceptions under Title I and Title II differ. The provider exception under Title I allows interceptions on a limited basis to cover interceptions that are necessary to provide the communications service. However, Title II’s exception is broader and entirely exempts “the person or entity providing a wire or electronic communications service.”<sup>260</sup> The wording of the consent exceptions under Title I and Title II also differs, with Title I requiring consent and Title II requiring authorization. However, this difference in wording has not lead to different interpretations of the nature of consent required for the Title I and Title II exceptions. Generally, the exceptions require consent to be given by one party to the

---

255. 18 U.S.C. § 2511(2)(a)(i) (2000) (providing that a communications service provider may “intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service.”).

256. See 18 U.S.C. § 2511(c) (2000); see also SOLOVE ET AL., *supra* note 29, at 269 (“For example a person can secretly tap and record a communication to which that person is a party”).

257. See Lasprogata et al., *supra* note 28, at ¶73; see also *Fischer v. Mt. Olive Lutheran Church, Inc.*, 207 F. Supp. 2d 914, 922-23 (W.D. Wis. 2002) (holding the interception of an employee’s telephone conversation was not exempt under Title I because it was not a business call and monitoring a personal call was not justified by valid business concerns).

258. 18 U.S.C. § 2701(c)(1). See also 18 U.S.C. § 2702(b).

259. See Lasprogata et al., *supra* note 28, at ¶ 73; see also *Fischer*, 207 F. Supp. 2d at 925-26 (holding that an employer’s access of an employee’s off-site email account (one not provided by the employer) may violate Title II of the ECPA because it was not covered by any exception); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 876-79 (9th Cir. 2002) (holding that an employer’s unauthorized access of an employee’s nonpublic and off-site Web site without authorization may also violate Title II).

260. 18 U.S.C. § 2701(c)(1) (2000); see also SOLOVE ET AL., *supra* note 29, at 271.

communication for a third party to intercept or access the communication, and both express and implied forms of consent are acceptable, including implied consent based on a policy or user agreement.<sup>261</sup> In contexts involving workplace monitoring of email systems, these two consent exceptions have been found to shield a broad array of workplace monitoring by employers based on employees' consent inferred from imposing a workplace policy that notifies employees of their employer's reservation of monitoring rights with respect to wire or electronic communications in the workplace and on company equipment.<sup>262</sup>

From an m-advertising perspective, one important limitation of the ECPA's privacy protections is that it only protects the contents of electronic communications from unlawful interception or access; it does not broadly protect consumers' information privacy with respect to their personal data.<sup>263</sup> Clearly, addressing information used to generate mobile advertising messages would not be protected by the ECPA, so the ECPA would not restrict advertisers' use of mobile phone users' names, addresses (email or postal), and their mobile phone numbers. However, the words spoken by the parties in a mobile telephone conversation are clearly contents of an electronic communication that are protected by the ECPA from unlawful interception or access and from further disclosure, unless one of the exceptions applies.<sup>264</sup> Both the provider and consent exceptions under Title I and Title II will likely shield monitoring by mobile telecommunications carriers and, because carriers are providers of wireless communications systems, the provider exceptions will apply. Further, the ECPA's consent exceptions are likely to be broadly construed to permit m-advertisers to obtain consent in a variety of ways, including subscription agreements between consumers and mobile carriers that may authorize carriers and third party advertisers to send mobile advertising to consumers. It is also likely that consumers will be asked to consent to online agreements as a precondition to accessing Web sites from their mobile

---

261. Serena G. Stein, Note, *Where Will Consumers Find Privacy Protection from RFIDS?: A Case for Federal Legislation*, 2007 DUKE L. & TECH. REV. 3, ¶¶ 38-39 (2007).

262. See Nancy J. King, *E-Mail and Internet Use Policies*, in 3 HANDBOOK OF INFORMATION SECURITY 908, 908-26 (Hossein Bidgoli, ed., 2006).

263. See 18 U.S.C. § 2510(4) (2000) (defining an "intercept" of a communication as acquiring its content through use of any "electronic, mechanical, or other device"); see also SOLOVE ET AL., *supra* note 29, at 268 ("The classic example of an activity covered by [Title I of the ECPA] is the wiretapping of a phone conversation – a device is being used to listen to a conversation as it is occurring, as the words are moving through the wires.").

264. Addressing or transactional data related to electronic communications is not protected by the ECPA's prohibitions on interception or unauthorized access of electronic communications because it is not considered to be contents of electronic communications. See Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1114 (2002).

devices. Legally these agreements seem similar to the click-through agreements required for consumer to access content using their Internet browsers on traditional Web sites. Such agreements may require consumers to give their consent to receive m-advertising and/or for the advertiser to collect, use, and disclose the consumers' personal data, in exchange for being granted access to the .mobi Web site content or other services.

Some aspects of application of the ECPA to mobile communications are not yet clear. For example, it is not yet clear whether the wiretapping and interception provisions of Title I apply to interception of location tracking data related to mobile phone users.<sup>265</sup> Further, Title II's prohibitions on unauthorized access to stored communications must also be examined to determine if Title II restricts access to location information in computer storage about mobile phone users' locations.<sup>266</sup> If the ECPA does not protect mobile phone call location data, other federal laws that regulate the use of pen registers and trap and trace devices may provide some measure of consumer privacy protection, and they too must be examined to determine if they protect call location information.<sup>267</sup> These laws may still be important to protect consumer privacy from interceptions and unauthorized access, especially in situations where FCC regulation may not apply, such as privacy invasive m-advertising practices by third parties that are not FCC regulated carriers.

## VI. STATE PRIVACY LAWS AND M-ADVERTISING

State laws may supplement federal laws that regulate m-advertising and protect consumers' privacy. These laws include state consumer protection legislation and common law contract and tort laws.

---

265. See *Lee, supra* note 43, at 395 (explaining that the ECPA grants certain privacy protections to electronic communications under § 2510(12), but subsection C explicitly excludes from this definition "any communication from a tracking device" and that another section of the ECPA does address "mobile tracking devices," which are defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object"). Whether this definition covers call location information related to mobile phones is not certain.

266. See generally Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2711 (2000). The SCA regulates the government's ability to require electronic communication service providers or remote computing service providers to disclose "the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber." See 18 U.S.C. § 2703(c)(2) These provisions do not specifically address wireless location information. See *Lee, supra* note 43, at 398.

267. See 18 U.S.C. §§ 3121-3127 (2000) (prohibiting any person from installing or using a pen register or a trap and trace device without first obtaining a court order). These provisions may not apply to tracking devices that track a mobile phone user's geographic call location since they refer to "numbers dialed or otherwise transmitted" on telephone lines. See *Lee, supra* note 43, at 396.

### *A. State Consumer Privacy Laws Address Unfair and Deceptive M-Advertising Practices*

Some states have passed state consumer protection legislation that supplements federal consumer protection statutes including those enforced by the FTC. Therefore m-advertisers may face different or stiffer state regulation of their m-advertising practices that vary depending on where the advertisers operate. Regarding the FTC's Telemarketing Sales Rule ("TSR"), Verizon Wireless commented on the diversity of state consumer protection laws that apply to telemarketing companies and that go beyond federal regulation of telemarketing activities and asked the FTC to restrain state regulation that imposes divergent requirements on telemarketers.<sup>268</sup> As summarized by Verizon Wireless:

Currently, a majority of states that have telemarketing laws impose requirements which vary from or exceed the scope of those set forth in the TSR. The varying state requirements relate to, among other things, the manner in which a telemarketer's dialogue may be conducted (i.e., the means by which telemarketers are permitted to supply information and respond to consumer inquiries), licensure requirements of telemarketing salespersons, the types of organizations which are exempt from telemarketing rule requirements, the times within which telemarketing solicitations may be made, and the binding nature of purchase commitments made through telephone sales.<sup>269</sup>

In its comments, Verizon went on to summarize some of the specific state telemarketing laws that impose more onerous requirements on telemarketers:

[F]or example, Alabama, Connecticut, Florida, Kansas, Kentucky, Maine, Maryland, North Dakota, and Ohio require a signed contract for the sale to be valid. At least three of these states also demand that the consumer return the signed agreement to the telemarketer before the telemarketer can process payment. Kentucky and North Carolina require a telemarketer to ask the called party if they are eighteen years of age or older before the telemarketer is able to continue with the call. Furthermore, five states require that the telemarketer request permission to continue with the solicitation at the outset of the call, and eight states require that the telemarketer end the call immediately if the consumer gives a negative response or indicates no interest in the solicitation.<sup>270</sup>

It argued that divergent state regulation of telemarketing practices serves to confuse individuals and companies alike and makes compliance difficult for companies that conduct business throughout the United States

---

268. See Verizon Comments on the TSR, *supra* note 68.

269. *Id.*

270. *Id.*



while offering little, if any, additional protection to consumers beyond what is already available through the federal TSR.<sup>271</sup>

### *B. Common Law Privacy Torts May Apply to M-Advertising Practices*

Four privacy tort theories are currently recognized by the courts in most American jurisdictions.<sup>272</sup> These four tort theories are: 1) unreasonable intrusion upon the seclusion of another, 2) appropriation of another's name or likeness, 3) giving unreasonable publicity to another person's private life, and 4) publicity that unreasonably places another person in a false light before the public.<sup>273</sup> Of these four, the tort of unreasonable intrusion into seclusion is the most promising theory for customers seeking to recover damages from telecommunications carriers or m-advertisers based on claims that the customers' rights to privacy have been breached.<sup>274</sup> Unreasonable intrusion claims generally require the plaintiff to show that she had a reasonable expectation of privacy and that the defendant unreasonably intruded into her privacy.<sup>275</sup> The privacy torts provide a litigation avenue to recover damages for persons whose data privacy has been breached by a private person, a business, or the government,<sup>276</sup> although plaintiffs face stiff obstacles to recovery for data privacy breaches, as explained below.

---

271. *Id.*

272. See Benjamin E. Bratman, *Brandeis and Warren's The Right to Privacy and the Birth of the Right to Privacy*, 69 TENN. L. REV. 623, 624 (2002).

273. *Id.* See also RESTATEMENT (SECOND) OF TORTS § 652A-E (1977); WILLIAM PROSSER, LAW OF TORTS 802-18 (4th ed. 1971).

274. See e.g., Don Corbett, *Virtual Espionage: Spyware and the Common Law Privacy Torts*, 36 U. BALT. L. REV. 1, 25-26 (2006) (commenting, for example, that intrusion into seclusion is the most viable avenue for spyware claims, which often involve intrusive forms of advertising practices).

275. See *id.* at 25-27; see also McLaren v. Microsoft Corp., 1999 Tex. App. LEXIS 4103 \*9 (Tex. Ct. App. 1999) (discussing the tort of unreasonable intrusion into privacy, which requires the plaintiff to prove that the defendant intentionally intruded, physically or otherwise, upon the plaintiff's solitude or seclusion or private affairs or concerns and that the intrusion would be highly offensive to a reasonable person).

276. A plaintiff may recover damages under the privacy torts without proving any actual injury, such as mental distress. Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 965 (1989). For data privacy breaches that occur in m-commerce or m-advertising, the tort of unreasonable intrusion may be an applicable tort theory. Mobile phone users may perceive the receipt of unwanted mobile advertising on their cell phones as unwarranted use of their personal data and invasions of their privacy. However, this tort theory has limitations as a mechanism to address data privacy breaches because it does not apply to information that is already public, such as personal information that is already in the public record. Susan E. Gindin, *Lost and Found In Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1189 (1997) (noting, however, liability would likely be imposed for unauthorized access to or interception of electronic communications). Arguably, cell phone

U.S. privacy tort law is state common law, and it has evolved to a limited extent to protect data privacy.<sup>277</sup> This has occurred under the common law system as courts have applied common law privacy doctrines to resolve data privacy claims. For example, *Doe v. High-Tech Institute*<sup>278</sup> involved personal data privacy intrusions related to medical testing by a school and subsequent disclosure of the results of the testing to a government agency.<sup>279</sup> The Colorado Court of Appeals held that the student had two separate causes of action against the school based on privacy tort law to address the collection and disclosure of his private medical information. First, he had a cause of action for unreasonable intrusion into his privacy based on allegations that the school conducted unauthorized medical tests on his bodily fluids beyond the specific medical test he had authorized.<sup>280</sup> Second, he had a cause of action for impermissible public

---

numbers are in the public record since mobile phone companies must disclose them to the FCC, although as yet, telecommunications carriers have not issued a wireless phone directory. See *supra* note 218. Further, many consumers' cell phone numbers may be otherwise available as they are collected by m-advertisers from consumers and/or become included in commercial databases. For a discussion of the public availability of consumers' mobile phone numbers, see *infra* notes 372-373. Nor is there liability for this tort if the intrusion occurs in a public space where the data subject cannot reasonably expect privacy. See Ginden, *supra*, at 1189. Arguably, consumers' mobile phone conversations and cell phone numbers are communicated in public space to the extent that radio waves in public space are utilized. Further, to recover damages for the tort of intrusion, consumers bringing civil suits must show that the data privacy breaches of which they complain of would be offensive to a reasonable person. See Eden, *supra* note 49, at n.21.

277. Tort law in the United States originated as part of the common law system. See generally, FRIEDMAN, *supra* note 51, at 1, 4. Generally, the common law evolved on a case by case basis in judicial decisions in state court cases rather than through legislation. *Id.* Researching state tort law through reported judicial opinions is a difficult task since there are multilevel state courts in the fifty states of the United States. To make this task easier, the American Law Institute publishes *Restatements of the Law* that compile common law doctrines and case references, including state tort law, and these treatises provide a summary of the common law rules followed by the courts in most states. American Law Institute, About the American Law Institute, at <http://www.ali.org/ali/thisali.htm> (last visited June 22, 2007). The *Restatement (Second) of Torts* is a secondary authority of state tort law, with the primary authority of the law being found in state statutes and court opinions, but it is a highly regarded authority that is often used and referenced by judges in their opinions. See Tracie B. Loring, *An Analysis of the Informational Privacy Protection Afforded by the European Union and the United States*, 37 TEX. INT'L L.J. 421, 428 (2002). As courts decided cases involving torts (civil claims of damages for wrongful injuries to persons or property), a body of case law was created that contained the common law tort doctrines. See FRIEDMAN, *supra* note 51, at 143.

278. *Doe v. Hi-Tech Inst., Inc.*, 972 P.2d 1060 (Colo. 1998).

279. See *id.* at 1065-66. In this case, the school obtained consent from a student to test his blood for rubella. The school then performed an additional test without the student's consent to confirm that the student had the human immunodeficiency virus (HIV). After obtaining the student's test results, the school disclosed the student's HIV-positive status to a government department of health.

280. *Id.* at 1071 (holding that "[a]n unauthorized HIV test, under the circumstances as set forth in plaintiff's complaint, would be considered by a reasonable person as highly

disclosure of private facts based on allegations that the school improperly disclosed his medical test results to a government agency.<sup>281</sup> It is likely significant that the privacy claims in this case involved highly sensitive medical testing for HIV.<sup>282</sup>

However, as a vehicle to address data privacy concerns of consumers related to their mobile phones, state tort law has serious limitations, as cell phone customers learned in a recent class action lawsuit brought against Motorola, a cell phone carrier.<sup>283</sup> In *Busse v. Motorola*, customers claimed that Motorola invaded their privacy by intruding into their seclusion by passing on personal information to a third party, Epidemiology Resources, Inc. ("ERI"), without the customers' permission, for ERI's use of the information in a study of cell phone safety.<sup>284</sup> The types of customer personal data released by Motorola to ERI included customers' names, street addresses, cities, states, zip codes, dates of birth, social security numbers, wireless phone numbers, account numbers, start of service dates, and the unique electronic serial numbers of the customers' phones.<sup>285</sup>

Where some information was missing from that provided by Motorola, ERI obtained it through a contract with TRW, a credit bureau.<sup>286</sup> ERI used the customers' data to generate an email survey that was sent to Motorola's customers as part of a study to investigate possible links between wireless telephone use and mortality, although the customers were not told in the survey that the survey was designed to measure cell phone safety.<sup>287</sup> On defendants' summary judgment motion, the court dismissed the customers' claims of invasion of privacy for unreasonable intrusion because the court held that plaintiffs could not prove a required element of their case, and that defendants intruded on "a private matter or private facts."<sup>288</sup> According to the court, for the plaintiffs to recover for this tort:

---

invasive, and therefore, is such sufficient to constitute an unreasonable or offensive intrusion").

281. *Id.* at 1068.

282. *Id.* at 1071.

283. *Busse v. Motorola, Inc.*, 813 N.E.2d 1013, 1013 (Ill. App. Ct. 2004).

284. The plaintiffs (cell phone customers of Motorola) also alleged that Motorola breached its contract with its customers when information received from the customers was passed on to a third party without permission and then used to study cell phone safety. *See id.* at 1014. The contract law aspects of the decision are discussed *infra* Section VI.C.

285. *Id.* at 1015.

286. *Id.*

287. *Id.* The email survey asked customers questions about how many minutes they talked on their cell phones per week, which ear did they most often hold their cell phones against, and how often the customers shifted their cell phones from ear to ear while talking. Results of the study were published but individual customers were not identified in the published study. *Id.*

288. *Id.* at 1017.

Private facts must be alleged. Without private facts, the other three elements of the tort need not be reached. Because the analysis begins with the predicate, private facts, it also ends there if no private facts are involved. Here, none of the “personal” information furnished by the customers, standing alone – names, telephone numbers, addresses or social security numbers – have been held to be private facts.

....

In the absence of an Illinois law defining social security numbers as private information, we cannot say that defendants’ use of this number fulfills the privacy element necessary to plead intrusion upon seclusion. Nor are the individual pieces of information – names, address, particulars of cell phone use – facially revealing, compromising or embarrassing.<sup>289</sup>

Because both the tort of unreasonable intrusion into seclusion and the tort of public disclosure of private facts require the plaintiff to prove private facts that underlie the claimed privacy invasion, courts are unlikely to apply these torts to address consumers’ privacy claims associated with commercial surveillance or other collection and use of consumers’ personal data in m-advertising transactions.<sup>290</sup> To the extent that a consumer has given their mobile phone number to someone who uses it for m-advertising purposes, even if the m-advertiser sells it to another business for marketing purposes or contributes the mobile phone number to a commercial database, it is unlikely that the consumer will be able to show these actions involve private facts or that she had a reasonable expectation of privacy with respect to her personal information. Alternatively, the receipt of m-advertising or use of consumers’ personal data for m-advertising will not likely be considered an unreasonable intrusion into one’s privacy, even if it is annoying to consumers.

Regarding use of the tort of disclosure of private facts, to be actionable, the private facts disclosed by a commercial entity from the consumer must be of an intimate and sensitive nature.<sup>291</sup> This requirement may make the tort theory of little use to consumers arguing that collection of personal data about their mobile phone numbers or consumption habits with respect to their mobile phones (e.g., Web sites visited and purchases

---

289. *Id.* at 1017-18. The court’s analysis gave particular attention to whether the customers’ social security numbers were private information, concluding that they were not, although it recognized that in some jurisdictions, social security numbers have been recognized as confidential and private. *See id.* at 1018. The court listed the elements of this cause of action as recognized in this state to require plaintiff to prove: “(1) the defendant committed an unauthorized intrusion or prying into the plaintiff’s seclusion; (2) the intrusion would be highly offensive or objectionable to a reasonable person; (3) the matter intruded on was private; and (4) the intrusion caused the plaintiff anguish and suffering.” *Id.* at 1017.

290. *See id.* at 1017-18; Corbett, *supra* note 274, at 23 (commenting that “intrusion upon one’s seclusion and public disclosure of private facts both necessitated the invasion of something confidential”).

291. Eden, *supra* note 49, at n.20.

made using Internet-enabled mobile phones) is objectionable enough to be protected by this tort theory.<sup>292</sup> Those arguing that this type of information is not intimate or sensitive may point out that consumers themselves provide their mobile phone numbers in mobile commercial transactions. Further, in m-commerce, consumers' mobile consumption habits are observed and recorded while they are visiting Web sites with their mobile phones, which is analogous to making observations of consumers' public behavior in brick and mortar retail shops, and thus no reasonable expectation of privacy should attach to information about consumers' mobile consumption habits.

On the other hand, m-advertisers' collection, use, or disclosure of other types of personal data may be more likely to be protected under this theory because it is significantly more intimate and sensitive, at least from the consumers' viewpoint. For example, personal data that reveals the geographic locations of mobile phone users at specific times may be sufficiently sensitive and intimate in that it would allow m-advertisers to track consumers' activity from place to place—tracking that may perhaps be viewed by consumers as “commercial stalking.” To assess an intrusion into seclusion claim brought by consumers' against m-advertisers for location tracking, courts would consider whether the m-advertiser's behavior “transgressed the kind of social norms whose violation would properly be viewed with outrage or affront.”<sup>293</sup>

Arguably, subjecting the mobile phone user to tracking in a geographic area to generate unsolicited m-advertising would not reach this level of transgression as it is difficult to distinguish these advertising practices from other forms of common and lawful commercial advertising behavior, like commercial advertising practices that generate junk mail and email spam.<sup>294</sup> There is one important distinction, however, between advertising practices that involve sending junk mail and email spam and those that are directed at mobile phones. In the case of m-advertising

---

292. See *supra* note 289.

293. Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 962 (1989).

294. See *Cent. Hudson Gas & Elec. Corp. v. Public Serv. Comm'n*, 447 U.S. 557, 563-64 (1980) (holding that the First Amendment protects “the informational function of advertising,” however, governments are free to regulate commercial messages that are untruthful or illegal and may “ban forms of communication more likely to deceive the public than to inform it”); *Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 68-69 (1983) (holding that the burden of discarding unsolicited “junk” mail is minimal and does not outweigh commercial speech protections); *Rowan v. U.S. Post Office Dep't*, 397 U.S. 728, 736 (1970) (stating that “the right of every person to be let alone must be placed in the scales with the right of others to communicate,” and holding that an opt-out statutory requirement for sexually provocative mail advertisement is a constitutional restriction on commercial speech).

practices that involve unsolicited calls and text messages to mobile phones, federal telemarketing rules requires the sender to obtain the consumers' consent in advance of generating these forms of advertising if autodialed or sent using a wireless Internet domain name on the FCC's official list, so presumably federal law recognizes that consumers have heightened privacy protections related to personal data associated with their mobile phones.

It may be that courts will find that tracking mobile phone users' locations in order to generate m-advertising falls within the tort of unreasonable intrusion into consumers' seclusion to the extent that location tracking is involved and consumers have not consented to the practice. Essentially, location tracking by m-advertisers is a form of electronic surveillance or monitoring and it is possible to conduct this surveillance without the consumers' knowledge or consent.<sup>295</sup> Courts have applied the tort of unreasonable intrusion into seclusion to electronic monitoring.<sup>296</sup> It is the unreasonableness of the intrusion into peoples' privacy that is protected by this tort, not whether or not the use of the information obtained by the monitoring was reasonable.<sup>297</sup>

### *C. Common Law Contract Principles May Limit or Facilitate M-Advertising Practices—Focus on Mobile Services Agreements*

As Daniel Solove writes, contracts often function "as a way of sidestepping state and federal privacy laws."<sup>298</sup> In the context of m-advertising, telecommunications carriers and m-advertisers may seek to enter into contracts with consumers that are designed to satisfy the carriers' or m-advertisers' obligations to comply with federal or state consumer privacy laws that protect consumers' privacy and personal data. Subscriber agreements between telecommunications carriers and their customers are contracts governed by state contract law as well as federal and state consumer protection laws previously discussed. Likewise, m-advertisers

---

295. See Corbett, *supra* note 274, at 27 (making the argument that spyware loaded onto a user's computer without their knowledge or consent and used by advertisers to collect personal information about the user including their Web surfing habits is a form of electronic monitoring or electronic surveillance). By analogy, location tracking of consumers for m-advertisers without their knowledge and consent can be viewed as a form of spyware; when tracking of mobile phone users' locations and other behavior is conducted without notice and consent, it may also be viewed as an unreasonable intrusion into the seclusion of mobile phone users. See *id.*

296. See Corbett, *supra* note 274, at 27-29 (summarizing cases where surveillance tools have been deemed to violate a plaintiff's privacy rights even where the defendant did not physically intrude into or trespass on plaintiff's private property).

297. See *id.* at 28.

298. SOLOVE ET AL., *supra* note 29, at 32 (explaining, for example, that "[m]any employers make employees consent to drug testing as well as e-mail and workplace surveillance in their employment contracts").

(businesses that may or may not also be telecommunications carriers but that engage in mobile advertising directed at consumers) may also enter into contracts with consumers that will also be governed by state contract law and federal and state consumer protection laws.

Some of the general types of contractual clauses that may be included in subscriber agreements or in various agreements drafted by m-advertisers to be entered into with consumers include: 1) clauses that acknowledge consumers' consent to receive m-advertising or authorize the carrier or m-advertiser to use the consumers' personal data to generate advertising or for other purposes, 2) clauses that attempt to obtain consumers' waiver of federal or state consumer privacy rights or remedies related to m-advertising or other uses of consumers' personal data, and 3) clauses that attempt to obtain agreements from consumers to arbitrate any privacy or data protection claims rather than litigate these claims in the courts.

Where these types of contractual provisions are enforceable in the courts, they may serve to reduce mobile telecommunication carriers' or m-advertisers' risk of violating consumers' federal or state privacy rights. More importantly, to the extent that such agreements are enforceable, the agreements may serve as a mechanism for carriers and m-advertisers to comply with their consumer privacy obligations. For example, an agreement between a telecommunications carrier and its subscribers for mobile phone services may authorize the carrier to send advertisements to its subscribers' mobile phone numbers. This type of agreement may also authorize the carrier to use or release the customers' mobile phone numbers and other personal data for the purpose of enabling the carrier or third parties (e.g., advertisers) to direct advertising to customers' mobile phone numbers.<sup>299</sup> Further, as a condition of participating in m-commerce, consumers may be required to enter Web site access agreements and/or to acknowledge privacy policies that are designed to obtain consumers' consent authorizing m-advertisers to collect, use, and disclose consumers' personal information.<sup>300</sup> Conceivably, personal data collected for m-

---

299. The federal statutory requirements that limit the use of a subscriber's CPNI and subscriber list information only apply to telecommunications carriers that are regulated by the FCC. See *supra* notes Section V.D. Web site operators, m-advertisers, and other noncarriers are not required to comply with these rules.

300. See Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN. ST. L. REV. 587, 590-611 (2007) (describing the way personal information is provided by Web site visitors and the nature of privacy policy terms); see also Daniel D. Barnhizer, *Propertization Metaphors for Bargaining Power and Control of the Self in the Information Age*, 54 CLEV. ST. L. REV. 69, 75-82 (2006) (discussing characteristics of consumer contracting in the information age including heightened disparities in bargaining power between consumers and sellers).

advertising purposes may include wireline or mobile phone numbers and location data.<sup>301</sup>

U.S. contract law is essentially state law and thus varies from state to state.<sup>302</sup> As in the case of state tort law, court opinions examining contract law theories are an important source of common law doctrines and statutory interpretation related to state contract law.<sup>303</sup> Both parties to a contract must manifest their assent to the contracts terms for the contract to be enforceable.<sup>304</sup> The requirement of assent to form a binding contract applies to the enforceability of consumer consent provisions in subscription agreements and online privacy policies.<sup>305</sup> Generally, consumers are bound by the terms of these agreements if they have signed, "clicked," or otherwise signified acceptance of the terms and have actual notice of the terms.<sup>306</sup> Typical consumer contracts for telecommunications service or m-advertising may be characterized as form or adhesion contracts that are generally drafted by the carrier or the m-advertiser under circumstances where the consumer has little bargaining power to negotiate the terms of the agreement.<sup>307</sup> At least theoretically, defenses to enforcement of contracts, such as the defense of unconscionability, may limit the enforceability of clauses in services agreements, Web site access agreements, etc., that are too one-sided or unfair to the consumer.<sup>308</sup> Courts

---

301. See Haynes, *supra* note 300, at 605 (discussing recent federal and state enforcement actions brought against companies that have failed to comply with their online privacy policies, including an action against Yahoo! for making a promise in its privacy policy not to share telephone numbers but then announcing that its privacy policy was being amended to allow sharing such numbers). To resolve the state enforcement action, Yahoo! agreed not to share the numbers or misuse them. *Id.*

302. See generally RESTATEMENT (SECOND) OF CONTRACTS (1981) (summarizing the common law of contracts, which governs services contracts, real estate contracts and other contracts that do not relate to the sale of lease of goods).

303. *Id.* (providing references to court cases that have applied and interpreted the state common law of contracts).

304. See Haynes, *supra* note 300, at 613.

305. See *id.*

306. See *id.* at 614.

307. See FRIEDMAN, *supra* note 51, at 382 (discussing a form of consumer contract known as an adhesion contract, which is "a form contract – a take-it-or-leave-it contract – almost always drafted by business lawyers, to be signed by customers who never read the "fine print"). See Haynes, *supra* note 300, at 619 (discussing the growing use of "standard form" contracts with boilerplate provisions).

308. See FRIEDMAN, *supra* note 51, at 383. The doctrine of unconscionability has been incorporated into the Uniform Commercial Code ("UCC"), which applies to contracts for the sale of goods, but courts have broadened the concept and applied it in other situations including contracts for services governed by common law. See *id.* The doctrine of unconscionability has been used by courts "to police unfairness or one-sidedness in a variety of contract terms," however, "[m]ost states require a showing both of procedural and substantive unconscionability in order to refuse enforcement of a contract term". Haynes, *supra* note 300, at 619.



have discretion to sever unconscionable clauses from contracts and to enforce the remainder of the contract rather than to invalidate the entire contract.<sup>309</sup> Additionally, federal or state consumer protection statutes may limit the enforceability of contractual terms in a services agreement or m-advertisers' agreement that violate consumers' rights under consumer protection laws.<sup>310</sup> Significantly, given this Article's focus on m-advertising, it does not appear that federal law would prevent a telecommunication carrier from obtaining "opt-in" consent of subscribers in a form mobile services agreement between subscribers and the carrier that would allow the carrier to release location data to its joint venture partners or independent contractors.<sup>311</sup> Thus state contract law would facilitate mobile carriers' compliance with the "opt-in" consent rules under federal law, so that other businesses who are in a contractual relationship with the carriers could lawfully use location data obtained from mobile carriers to send location-specific m-advertising to subscribers.

The inclusion of arbitration clauses in subscriber agreements is one way that telecommunications carriers may try to limit litigation costs and potential liability related to the use or release of customers' CPNI and other personal data (such as subscribers' cell phone numbers) for m-commerce purposes. Despite the typical unequal bargaining positions of telecommunications carriers and consumers, telecommunications carriers have successfully enforced arbitration clauses in subscriber agreements to compel arbitration by consumers who have a dispute and this is so even when consumers argue that federal consumer protection statutes have been violated. For example, in litigation involving claims that a telecommunications carrier violated its duties under the Federal Communications Act to protect the confidentiality of CPNI related to its wireless customers, the telecommunications carrier was able to move these

---

309. *Id.*

310. *See, e.g.,* Haynes, *supra* note 300, at 621-22 (stating that "a consumer may attempt to challenge as unconscionable other privacy terms that are inconsistent with FTC fair information practices, such as an inability to access personal information or control its use"). However, federal statutes may also be used by courts to find a carrier's privacy-intrusive practices are not a breach of contract with the carrier's subscribers to the extent that the statute permits the carrier to use subscribers' personal information. *See, e.g.,* Busse v. Motorola, 813 N.E.2d at 1016-17 (holding that the defendants (including Motorola, a mobile carrier) were entitled to judgment as a matter of law on plaintiffs' breach of contract claim). The court held defendants' passing of subscribers' personal data to third parties, without subscribers' permission and for use in a study of cell phone safety, was permitted under the federal Telecommunications Act of 1966, and thus did not breach the carrier's contract with its cell phone customers). *Id.*

311. *See* the discussion of location data as a form of CPNI protected by federal law and the discussion of "opt-in" consent required by the new 2007 CPNI Order, *supra* Section V.D. *See also* the discussion of the notice and consent requirements to send MSCMs, *supra* Section V.B.

claims from a court to an arbitration forum based on its subscriber agreement with its wireless customers that included an arbitration clause.<sup>312</sup>

Further, arbitration was ordered even though the subscriber agreement limited the available remedies to the customer. Although the federal court compelled arbitration in this lawsuit brought by customers against AT&T,<sup>313</sup> the court retained jurisdiction to later determine if the limitations of remedies portion of the contract was unenforceable in light of the consumers' statutory remedies under the Communications Act.<sup>314</sup> Presumably, the court would exercise its discretion to decide this question if the consumer plaintiffs in the case successfully proved in the arbitration that AT&T violated their privacy rights under the Communications Act. However, courts have applied the unconscionability doctrine to refuse to enforce arbitration clauses that are too one-sided—for example, those that allow one party to change the agreement without prior notice or that contain language that is so one-sided as to make any promises in the agreement illusory.<sup>315</sup>

Now having examined the complex federal and regulatory system applicable to businesses participating in m-advertising, this Article will analyze whether the current laws are adequate to protect consumers' privacy.

## VII. IS FEDERAL PRIVACY REGULATION ADEQUATE TO PROTECT CONSUMER PRIVACY IN M-ADVERTISING?

Currently there are indications that advertising to cell phone customers will soon be increasing as new services are offered by wireless phone companies.<sup>316</sup> These advertisements are likely to include telemarketing calls, banner ads, video ads, and text messages directed at or delivered on or through consumers' cell phones.<sup>317</sup> Further, "[a]s cell phones

---

312. *Penberthy v. AT&T Wireless Servs., Inc.*, 354 F. Supp. 2d 1323, 1323-27, 1329 (M.D. Fla. 2005). In *Penberthy*, a customer claimed that AT&T released CPNI about the customer including phone numbers the customer had called on her wireless service and her new unlisted phone number to a convicted felon who had stalked the customer, thus giving him greater access to her whereabouts and causing her damages.

313. *Id.* at 1329 (holding that contractual limitation of statutory remedies and claims were matters to be considered by the arbitrator).

314. *Id.* at 1330.

315. See Haynes, *supra* note 300, at 620-22.

316. See discussion of recent advances in mobile commerce and mobile advertising in the United States, *supra* Section II. Most notable are the recent decisions by Sprint and Verizon to allow ads to appear on the content menus that subscribers see when they use their phones to search for information on the Internet, a form of mobile advertising referred to as "on-deck" advertising. Richtel, *supra* note 33.

317. See *id.*

increasingly add sophisticated features such as Web browsing ... the ads will grow more common."<sup>318</sup>

The very nature of the mobile phone gives operators information about their customers that Internet and television advertisers can only dream of having. Carriers know not just where their clients live, but where they are at the moment that the ad is seen, how much they spend on phone services, whom they call and when, their age and sex, what games and music they play on their phones – and how to bill them. People in the industry say they know that the personalized nature of cell phones is a double-edged sword: it is what makes the medium appealing to advertisers, but many people consider the medium too personal to be invaded by outside interests.<sup>319</sup>

Will new privacy and data protection legislation and industry self-regulation be needed to protect consumers in m-commerce with respect to m-advertising? What will be the role of company and industry self-regulation?

#### A. *Consumer Privacy and the Market Approach to Data Protection*

Privacy and data protection regulation in the U.S. has traditionally been minimized in favor of allowing the free market to operate along with its incentives for industry self-regulation.<sup>320</sup> The U.S. approach,

318. See Bob Keefe, *Cell Phones Poised to Become One More Ad-Driven Medium*, COX NEWS SERVICE, Sept. 12, 2006 (on file with author). See also Eric Sylvers, *Cell Phone Ads May Take Off Soon*, N.Y. TIMES, Feb. 14, 2007, available at [http://www.nytimes.com/2007/02/14/business/media/14adco.html?\\_r=2&adxnnl=1&oref=slogin&adxnnlx=1191603714-y5N/e1D6414ap3ZzzBWCgG&oref=slogin](http://www.nytimes.com/2007/02/14/business/media/14adco.html?_r=2&adxnnl=1&oref=slogin&adxnnlx=1191603714-y5N/e1D6414ap3ZzzBWCgG&oref=slogin). Sylvers reported:

Yahoo [ ] began displaying ads on Sunday on sites accessible to subscribers with advanced cell phones in 19 countries. Mobile phone users with data as well as voice subscriptions would see the ads when going to Yahoo's home Web page on their phones. They could then click on an ad to dial a company directly or to get more information and special offers.

The advertisers that Yahoo has signed up include Pepsi, Proctor & Gamble, Hilton, Nissan, Singapore Airlines, and Intel. The 19 countries include the United States, Brazil, Britain, France, Germany, Italy and India.

*Id.* Sylvers also stated:

Already, ads are creeping onto cell phones around the globe. At this rate, experts say, it will not be long before the 2.2 billion mobile phone users around the world consider it natural to tune into a 15-second spot before watching a video, sending a message or listening to a downloaded song between phone conversations.

*Id.*

319. Sylvers, *supra* note 318.

320. Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 501 (1995). According to Reidenberg, "the idea that the government should not intervene in the marketplace of ideas in the absence of compelling needs remains dominant." Instead of "government action, private relationships or private contracts, thus, become a principal source of regulation for information flows." *Id.* Cf. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423-28 (2000) (arguing that market-based approaches to information privacy undervalue data privacy by treating it as a mere "matter of individual taste, entitled

characterized as the market approach to data protection, has generated a focus on fair information practices and privacy policies.<sup>321</sup> In contrast, the “dignity approach” to regulating data privacy espoused in other parts of the world is consistent with the view that individuals have a fundamental right to maintain a sphere of privacy free from major invasions by businesses or the government.<sup>322</sup> The dignity approach to data privacy rejects the ideology driving the market approach to data protection that data privacy should be “freely alienable in a marketplace” in favor of legislation and government enforcement to protect individuals in situations where they

---

to no more (and often less) weight than preferences for black shoes over brown or red wine over white” and that data privacy has a more fundamental role: providing individuals with informational autonomy enabling them to grow as individuals and promoting vital diversity of speech and behavior); Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1137-40 (2002) (arguing that the regulation of data privacy needs to be re-examined in view of modern technology allowing access and aggregation of personal data that is subsequently combined by private and governmental entities to create digital biographies about individuals).

321. See Ciocchetti, *supra* note 56, at 66 (proposing a new federal law designed to make electronic privacy policies more effective that would require all commercial Web sites collecting PII from consumers to conspicuously post a compliant electronic privacy policy; arguing that adoption of this law would protect consumers’ PII and preserve transactional efficiency).

322. See Treaty establishing the European Community, Nov. 10, 1997, 1997 O.J. (C 340) 2, available at <http://eur-lex.europa.eu/en/treaties/dat/11997E/htm/11997E.html#0173010078> (recognizing the ECHR and requiring Members of the European Union to respect the fundamental rights guaranteed by the Convention). More recently, the Charter of Fundamental Rights of the European Union provides: “Everyone has the right to the protection of personal data concerning him or her.” Charter of Fundamental Rights of the European Union, art. 8, 2000 O.J. (C 364) 1 [hereinafter Charter]. The Data Protection Directive (95/46/EC) requires EU Member States to adopt data protection legislation regulating the processing of personal data and the free movement of such data. Council Directive 95/46, 1995 O.J. (L281) 31 [hereinafter Data Protection Directive]. The Data Protection Directive expressly refers to the fundamental rights of privacy that are contained in the above mentioned conventions and treaties and states the intention to regulate the processing of personal data consistent with these fundamental rights. *Id.* in Preamble (providing that “the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law”). Privacy as a fundamental right is also recognized in international law, but there is no specific recognition of data protection as a fundamental right similar to that found in the EU. See, e.g., International Covenant on Civil and Political Rights and its Optional Protocol, G.A. Res. 2200 (XXI), U.N. GAOR, 21st Sess., Supp. No. 16, U.N. Doc. A/6316 (1966) [hereinafter ICCPR]. See generally Nancy J. King, *Fundamental Human Rights Principle Inspires U.S. Data Privacy Law, But Protections Are Less Than Fundamental*, in DESAFIOS DEL DERECHO A LA INTIMIDAD Y A LA PROTECCION DE DATOS PERSONALES EN LOS ALBORES DEL SIGLO XXI. PERSPECTIVAS DEL DERECHO LATINAMERICANO, EUROPEO Y NORTEAMERICANO (forthcoming 2008) [Coordination, *Centre de Recherches Informatique Et Droit (CRID)*, University of Namur, Namur, Belgium and *Foro Habeas Data*, Buenos Aires, Argentina, Publishing House: Editorial Heliasta, Argentina].

have relatively less power than the companies and organizations that would collect and process individuals' personal data.<sup>323</sup>

Under the market approach to data privacy regulation used in the U.S., company-specific privacy policies play an important role in balancing the rights of consumers to protect the privacy of their PII with the rights of businesses to pursue transactional efficiencies that will enhance their competitive position in the marketplace.<sup>324</sup> Further, industry-adopted privacy policies and other mechanisms of industry self regulation are tools that may help achieve this balance.<sup>325</sup>

### *B. Privacy Policies Should Provide Notice and Disclose Company Privacy Practices*

Privacy policies are essentially statements of fair information practices that individual companies or an industry association of companies have promised to follow for the collection, processing, and distribution of individuals' PII.<sup>326</sup> In other words, privacy policies give notice or disclose an organization's privacy practices to affected individuals including consumers who are on the receiving end of m-advertising. The extent to which such a company-specific privacy policy complies with fair information principles advocated or adopted by various organizations is a measure of how well that policy is designed to protect the data privacy of individuals. Principles of fair information practices can be found in numerous sources including: 1) those set forth in legislation (like the principles enacted in national laws of countries in the European Union ("EU") that have implemented the EU's Data Protection Directive or the CPNI rules under the federal Communications Act and binding administrative rules in the U.S.);<sup>327</sup> 2) policy statements of government

---

323. See Ciocchetti, *supra* note 56, at 66.

324. See *id.* at 57.

325. *Id.* at 96-98 (discussing forms of industry self-regulation that involve voluntary actions by companies to provide fair information practices that protect consumer privacy and PII including the Platform for Privacy Preferences (P3P) and third-party enforcement programs). P3P is "software technology created to monitor Web site privacy policies ... [that was] developed ... to allow users of the Web to communicate their privacy preferences more effectively before the Web sites they visit can collect their PII." *Id.* at 97. In third-party enforcement programs, an "independent entity ... validate[s] the privacy practices of individual companies." *Id.* at 98. "The most recognized third-party enforcement programs today are the third-party seal—or Trustmark—companies. These companies certify that the company privacy policies meet certain minimum information-privacy standards like the FTC fair information practices of notice, choice, access, and security." *Id.* A third approach is for an industry association to adopt a code of conduct that sets minimum fair information practices to protect consumers' PII and that its members agree to follow.

326. Ciocchetti, *supra* note 56, at 68.

327. See generally Data Protection Directive, *supra* note 322. Fair information practices mandated by the Data Protection Directive include the following general principles: 1)

agencies that are advisory but not legally binding (like the U.S. FTC's fair information principles: notice, consent, access, security, and enforcement);<sup>328</sup> and 3) the principles announced by international organizations that are advisory but not legally binding (like the Organisation for Economic Cooperation and Development's ("OECD") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data).<sup>329</sup> Significantly, for the discussion in this section of the Article, each of these sources of fair information principles includes notions of meaningful notice and consent by the data subject to the use or disclosure of the data subject's personal data by any entity collecting the data.

There is growing consensus among privacy experts that complex privacy policies contained in a single document are not an effective way to communicate with consumers about the fair information processing practices of a business. Instead, privacy policies that feature more than one layer of consumer notices, from short notice forms to longer notice forms, are generally viewed as more effective methods to communicate privacy policies.<sup>330</sup> To satisfy the notice and disclosure component of fair information practices, companies should adopt privacy policies that are:

---

"purpose limitation" [legitimacy]; 2) "data quality"; 3) "data security"; 4) "sensitive data"; 5) "transparency"; 6) "data transfer to third parties"; 7) "independent oversight"; and 8) "individual redress." Tracie B. Loring, *An Analysis of Information Privacy Protection Afforded By the European Union and the United States*, 37 TEX. INT'L L.J. 421, 433 (2002). The principle of legitimacy for processing personal data requires the processor (data controller) to have the data subject's consent or show that processing is necessary to comply with a legal obligation or necessary to performance of a contract. Lasprogata et al., *supra* note 28, at ¶45.

328. FTC, Fair Information Practice Principles (1998) [FTC's FIP, 1998], available at <http://www.ftc.gov/reports/privacy3/fairinfo.shtm>. The second principle, Choice/Consent, includes obtaining consumer consent about how information collected from them may be used. *Id.*

329. Organisation for Economic Cooperation and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2001), available at [http://www.oecd.org/document/18/0,2340,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html) (last visited Jan. 31, 2008). See also Ciocchetti, *supra* note 56, at 61 n.26 (summarizing the OECD fair information practices to include these general principles: 1) collection limitation; 2) data quality principle; 3) purpose specification; 4) use limitation principle (which includes a restriction on use of the individual's personal data without the consent of the data subject or by the authority of law); 5) security safeguards principle; 6) openness principle; 7) individual participation principle; and 8) accountability principle).

330. See Ciocchetti, *supra* note 56, at 101 (arguing the "future of electronic privacy policies lies in a multilayered notice format rather than one long and complex document"). See also Center for Information Policy Leadership, Ten Steps to Develop a Multilayered Privacy Notice 1-9 (March 2007), available at [http://www.hunton.com/files/tbl\\_s47Details%5CFileUpload265%5C1405%5CTen\\_Steps\\_whitepaper.pdf](http://www.hunton.com/files/tbl_s47Details%5CFileUpload265%5C1405%5CTen_Steps_whitepaper.pdf) [hereinafter CIPL 10 Steps]; Martin Abrams, et al., Memorandum, Berlin Privacy Notices (April 2004), [http://www.hunton.com/files/tbl\\_s47Details/FileUpload265/681/Berlin\\_Workshop\\_Memorandum\\_4.04.pdf](http://www.hunton.com/files/tbl_s47Details/FileUpload265/681/Berlin_Workshop_Memorandum_4.04.pdf) [hereinafter Berlin Privacy Notices Memo].

1) *Multilayered*: Privacy notices should be provided in multilayered format, from short to longer layers of notice, with the most important information that consumers need to understand their positions and to make decisions included in the short notices and even shorter notice layers being perhaps acceptable for mobile phone screens and similar situations where space is limited;

2) *Comprehensible*: Privacy notices should be provided in a format that considers the ability of consumers to comprehend the meaning of the notice, using language that is easy for consumers to understand so that they can make informed decisions;

3) *Legally Compliant*: Privacy notices should be provided in a form that is legally compliant, such that all the layers taken together are compliant with relevant law and each individual layer communicates the information necessary to make an informed decision and avoids surprises by drawing attention to any processing that goes beyond established or expected norms;

4) *Consistently Formatted*: Privacy notices should be provided in a consistent format and layout to facilitate comprehension by consumers;

5) *Brief*: Privacy notices should be provided in a form that is brief, because research shows that consumers are only able to absorb a limited amount of information from the notice.<sup>331</sup>

Whether the notice is provided online or in paper form, according to privacy experts, a short initial privacy notice should be provided to the consumer that discloses:

- Who the privacy notice covers (i.e., who is the responsible person or entity);
- The types of information collected directly from the individual and from others about the individual;
- Uses or purposes for the processing;
- The types of entities that may receive the information (if it is shared);
- Information on choices available to the individual to limit use and/or exercise any access/or other rights, and how to exercise those rights; and
- “How to contact the collector for more information and to complain (to the collector and to an independent oversight body if appropriate).”<sup>332</sup>

---

331. See Berlin Privacy Notices Memo, *supra* note 330, at 2.

332. *Id.* (commenting that “[w]hile notices will be different from organization to organization and from sector to sector, similarity in format will facilitate individual knowledge and choices”). Focus group research related to U.S. consumers has shown that consumers prefer boxes with bold headings. *Id.* Also, in comparison to the short notices that

A third topic that is important for determining appropriate notice in privacy policies is the nature of the medium on which the privacy policy and relevant disclosures about the policy is to be made and on which the consumer will convey his or her consent. Currently, the viewing screen on most mobile phones is very small. Although some screens are getting larger, they are likely to be very small compared to the screen on a desktop or laptop computer. The possibility of using multilayered privacy policies, as opposed to a comprehensive standalone privacy policy, is especially relevant in this discussion of obtaining appropriate consent for m-advertising.<sup>333</sup> Models for short privacy notices that could be delivered on the screen of a mobile phone have been proposed, including one proposal that would provide only four lines of disclosure—it would simply notify the mobile phone user that: 1) the company has a privacy policy, 2) “We collect your information to market to you and to service your account,” 3) “You may tell us not to do so,” and 4) “View our complete privacy policy by calling [telephone number] or at [Web site address].”<sup>334</sup>

In theory, as companies and industries around the globe seek to follow the above five privacy policy drafting principles, consumers will increasingly be able to understand the terms of the privacy policies that they encounter. Consumers should also be able to exercise informed consent about the proposed processing of their personal information, including to what extent they are willing to permit unsolicited advertisements to interrupt their personal space.

### C. *Industry Models for Privacy Policies for M-Advertising*

A leading industry association in mobile advertising, the Mobile Marketing Association (“MMA”), promotes the adoption of a Code of Conduct for industry members that will include m-advertisers.<sup>335</sup> The

---

are the initial notices contemplated under the multilayered privacy approach, the additional complete notices would include all the details required by relevant laws. *Id.*

333. See Ciocchetti, *supra* note 56, at 101.

334. *Id.* at 102, Fig.1. See also Direct Marketing Association, DMA Policy Generators, <http://www.the-dma.org/privacy/privacypolicygenerator.shtml> (last visited Jan. 10, 2008).

335. See Mobile Marketing Association, About the MMA, <http://mmaglobal.com/> (last visited Jan. 10, 2008). The MMA is headquartered in the U.S. and has “400 members representing over twenty countries.” Its members include “agencies, advertisers, hand held device manufacturers, carriers and operators, retailers, software providers and service providers, as well as any company focused on the potential of marketing via mobile devices”). *Id.* See also Seventh ITU Internet Report, *supra* note 2, at 93 (describing proactive approaches of industry associations and individual companies to protect mobile users from the annoyance of unsolicited messages). The MMA defines mobile marketing as “the use of wireless media as an integrated content delivery and direct response vehicle within a cross-media marketing communications program.” Laura Marriott, *Mobile Marketing: Back to the Basics*, CLICKZ (Nov. 16, 2006), <http://www.clickz.com/showPage>



MMA's members include the full range of companies focused on the potential of marketing via mobile devices such as advertisers, handheld device manufacturers, and telecommunications carriers and operators, as well as retailers, software providers, and service providers.<sup>336</sup> The MMA's Code of Conduct is based on six categories: choice, control, constraint, customization, consideration, and confidentiality.<sup>337</sup> This code is an exercise of industry self-regulation that has a highly proconsumer privacy goal:

The Code provides consumers with the ability to opt-in and opt-out of receiving mobile marketing; it allows them to set limits on the type of messages received, based on their own preferences. To improve relationships between mobile operators and advertisers, the code compels its members to provide information of perceived value to the customer, to use analytical segmentation tools to optimize message volume and to align their privacy policies.<sup>338</sup>

Other industry associations may also play a role in establishing fair information practices for mobile commerce and mobile advertising to the extent that the associations adopt codes of conduct or privacy policies that their members commit to follow either directly or by adopting company-specific policies that are consistent with the industry association's code. For example, the Global System for Mobile Communications Association ("GSMA") is a global trade association representing hundreds of mobile phone operators (mobile carriers) and mobile phone manufacturers.<sup>339</sup> GSMA adopted a "Mobile Spam Code of Practice" ("Spam Code") to protect the secure and trusted environment of mobile services by ensuring that "customers receive minimal amounts of spam sent via SMS and MMS" (mobile message service or instant messaging).<sup>340</sup> The Spam Code only addresses mobile spam and does not purport to set fair information practices generally applicable to the collection, use, or disclosure of consumers' PII. Further, the Spam Code is only mandatory for those

---

.html?page=3623954. Mobile is viewed as one of many media channels to be integrated with other traditional and digital media elements such as print, on-pack, TV, and radio. *Id.*

336. See About the MMA, Mobile Marketing Association, *supra* note 335.

337. See Mobile Marketing Association, Code of Conduct for Mobile Marketing, <http://mmaglobal.com/modules/content/index.php?id=5> (last visited Oct. 6, 2007) [hereinafter MMA Code of Conduct]; see also Seventh ITU Internet Report, *supra* note 2, at 93.

338. Seventh ITU Internet Report, *supra* note 2, at 93.

339. GSM World, About GSM Association, <http://www.gsmworld.com/about/index.shtml> (last visited Nov. 10, 2007).

340. GSM Association Mobile Spam Code of Practice, (2006), [http://www.gsmworld.com/documents/initiative\\_flyers/mobile\\_spam\\_feb06.pdf](http://www.gsmworld.com/documents/initiative_flyers/mobile_spam_feb06.pdf). This code "takes a firm stance on how to deal with mobile spam messages that are either fraudulent or unsolicited commercial messages." *Id.*

members who have signed it.<sup>341</sup> However, in the context of mobile spam, it does require member operators who are signatories to the agreement to “[p]rovide a mechanism that ensures appropriate customer consent and effective customer control with respect to mobile operators’ own marketing communications.”<sup>342</sup>

The Near Field Communication Forum (“NFC”) is another industry association poised to play an important role in establishing fair information practices for mobile advertising. The NFC represents companies around the globe that are involved in near field communications technologies, and its members include mobile phone manufacturers and mobile carriers.<sup>343</sup> The incorporation of RFID technologies into cell phones and other mobile communications devices is an example of the type of privacy-implicating technologies that the NFC Forum will address.<sup>344</sup> The NFC has a privacy advisory council but has not yet adopted a privacy code of conduct for its members.<sup>345</sup>

Although much work has been done to define principles of fair information practices by industry associations and by governmental organizations that could serve as models for company-specific privacy and data protection policies, there is a gap between the theory and actually providing fair information practices.<sup>346</sup> Criticism of company-specific policies include arguments, some supported by empirical studies, that privacy policies are not read or understood by consumers and fail to provide meaningful consumer protections for PII, yet consumers assume that such policies do protect their privacy and personal data.<sup>347</sup> Critics also

---

341. *Id.*

342. *Id.*

343. See Near Field Communication (NFC) Forum, <http://nfc-forum.org/home> (last visited Nov. 10, 2007) (describing the NFC Forum as a global “non-profit industry association that promotes the use of NFC short-range wireless interaction in consumer electronics, mobile devices and PCs”).

344. See Near Field Communication (NFC) Forum, Near Field Communication White Paper: Near Field Communication and the NFC Forum, The Keys to Truly Interoperable Communications, NFC Forum (2006), available at [http://www.nfc-forum.org/resources/white\\_papers/nfc\\_forum\\_marketing\\_white\\_paper.pdf](http://www.nfc-forum.org/resources/white_papers/nfc_forum_marketing_white_paper.pdf) (last visited Nov. 10, 2007).

345. See Near Field Communication (NFC) Forum, Committees and Working Groups, [http://www.nfc-forum.org/aboutus/committees\\_and\\_wgs#pac](http://www.nfc-forum.org/aboutus/committees_and_wgs#pac) (last visited Nov. 10, 2007).

346. See, e.g., Haynes, *supra* note 300, at 610-611 (arguing that online privacy policies have become ubiquitous but have not resulted in real privacy protection for consumers and that “[w]e now have ten years of experience with privacy self-regulation online, and the evidence points to a sustained failure of business to provide reasonable privacy protections.”) (internal quotations omitted).

347. *Id.* at 611 (reporting on a survey that found seventy-five percent of consumers believed they had more privacy just because a Web site has a privacy policy and another survey that found consumers believed that the mere presence of a privacy policy meant the Web site could not share consumers’ personal information with third parties). See also Ciocchetti, *supra* note 56, at 69-70 (reporting that studies show Web site visitors are not

argue that companies recognize that consumers do not read or understand paper or electronic privacy policies. Consequently, some companies take advantage of consumers' failure to read or understand their privacy policies by failing to make any real promises of fair information practices in their policies or including privacy disclaimers that free the companies to do as they will with consumers' PII, even to the point of selling it to third parties.<sup>348</sup> To the extent that these policies are purely voluntary self regulatory efforts by companies or industry associations—meaning that the policies are not tools to communicate legally-required standards or there is no effective government enforcement of the standards—company-specific policies have failed to ensure fair information practices that protect consumers.

#### *D. Fair Information Practices for M-Advertising Must Include Obtaining Appropriate Consumer Consent*

As discussed in the previous section, fair information practices start with providing adequate notice and disclosure to consumers of the nature of the PII that the company collects about consumers and how the company will use that information. These disclosures are the basis for a company to obtain informed consent by consumers for collection, use, or disclosure of the PII and for the receipt of advertising initiated by m-advertisers, previously referred to in this paper as "appropriate consumer consent."<sup>349</sup> What are the components of consumer consent that should be included in a company-specific privacy policy for a company engaged in m-advertising in order to adequately protect consumers' privacy and their personal data?

The answer to this question begins with the recognition that there are two primary types of consent needed for m-advertising. First, the m-

clicking, reading, or understanding privacy terms and are not basing any decision on whether to continue on the Web site on the terms of the Web site's privacy policy).

348. See Ciochetti, *supra* note 56, at 69.

349. See generally FTC's FIP, 1998, *supra* note 328. This source offers the following guidance on the importance of providing notice and disclosure of a company's privacy policy to consumers with respect to collecting and using consumers' PII:

The most fundamental [fair information] principle is notice. Consumers should be given notice of an entity's information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information. Moreover, three of the other principles discussed below – choice/consent, access/participation, and enforcement/redress – are only meaningful when a consumer has notice of an entity's policies, and his or her rights with respect thereto.

Further, "[i]n order for consent to be meaningful . . . it must be informed. This has become increasingly difficult as technology outstrips the guidelines that govern it." Evelyne Beatrix Cleff, *Implementing the Legal Criteria of Meaningful Consent in the Concept of Mobile Advertising*, 3 COMPUTER L. & SECURITY REP. 262, 262-69 (2007) .

advertiser must obtain consent from consumers to have their PII collected and used, including consent to any further disclosure to third parties. Second, the m-advertiser must obtain consent from consumers signifying the consumer's willingness to receive m-advertisements on his or her mobile phones.

Dimensions of appropriate consumer consent include the timing ("opt-in" versus "opt-out") and level of specificity that should be required, whether consent is obtained under circumstances where the consumer has a choice, and the technological context in which consent is sought and obtained.<sup>350</sup> In terms of technological context, the discussion needs to consider the limitations associated with receiving, reading, and acknowledging privacy policies on mobile phones. For example, mobile phones currently have small screens, making it difficult for consumers to read privacy policies on their mobile phones. Further, mobile phone users are generally "on the go" and may not be inclined to read privacy policies closely because it would take too much time. Additionally, the wireless Internet access service that supports mobile phones may be a slow avenue for downloading privacy policies, and consumers may not have ready access to electronic storage or printers in order to retain a copy of the terms that they have viewed on their mobile phones. Appropriate consumer consent to receive m-advertising on mobile phones must address consumer privacy interests that go beyond the data protection concerns of m-advertisers' use of consumers' PII. Here such privacy concerns include interests that consumers have in being free from interruption by advertisements intruding on their work or social time because of the fact that consumers generally carry their mobile phones with them everywhere. Another privacy concern for consumers is being free to move unobserved in both public and private spaces, e.g., freedom from electronic surveillance by m-advertisers that is made possible by location tracking technologies that advertisers may use to generate personalized advertising for consumers based on their geographic locations at particular times.

---

350. See, e.g., FTC's FIP, 1998, *supra* note 328, at 2. The FTC explains the notion of choice/consent and the difference between "opt-in" and "opt-out" methods of consent:

[T]wo types of choice/consent regimes have been considered: opt-in or opt-out. Opt-in regimes require affirmative steps by the consumer to allow the collection and/or use of such information. The distinction lies in the default rule when no affirmative steps are taken by the consumer. Choice can also involve more than a binary yes/no option. Entities can, and do, allow consumers to tailor the nature of information they reveal and the uses to which it will be put. Thus, for example, consumers can provide separate choices as to whether they wish to be on a company's internal mailing list or a marketing list sold to third parties. In order to be effective, any choice regime should provide a simple and easily-accessible way for consumers to exercise their choice.

To analyze the nature of consent that should be obtained by m-advertisers before collecting their PII or sending consumers m-advertising, it is helpful to consider the different ways that m-advertising can be delivered on a mobile phone. There are several different ways that it is currently possible to deliver m-advertising to consumers' mobile phones. These include: 1) placing a mobile phone call to the consumers' mobile phone number (live, autodialed, etc.), 2) sending a text message to the consumers' mobile phone number (live, autodialed, etc.), 3) displaying advertising on a Web site visited by consumers using their Internet-enabled mobile phones (e.g., pop-ups, banners, etc.), 4) generating "on deck" advertising on the consumers' mobile phone handset (e.g., pop-ups, banners, etc., delivered by software installed on the mobile phone handset) perhaps raising privacy concerns similar to those raised by adware and spyware that has been loaded on a user's personal computer that is connected to the Internet.<sup>351</sup>

Another distinction that is relevant to the discussion of what constitutes appropriate consumer consent relates to whether the consumer or the m-advertiser initiates the delivery of m-advertising to the consumer. When the m-advertiser initiates the delivery of the advertisement to the consumer, this has been described as "push advertising."<sup>352</sup> Push advertising may be solicited or unsolicited, raising many of the same privacy concerns as traditional email advertising and spam. On the other hand, if the consumer requests a service using their mobile phone and the delivery of the service is accompanied by advertising, this has been described as "pull advertising."<sup>353</sup> It is "pull advertising" when a consumer uses his mobile phone to obtain a weather forecast from a .mobi weather forecast service provider and the weather forecast is delivered to the consumer's mobile phone, and the forecast is accompanied by a one-time advertisement.<sup>354</sup>

## 1. Using Form Agreements to Obtain Consumer Consent

Based on current practice, we can expect that m-advertisers will use form agreements to obtain consumer consent to the terms of their privacy

---

351. See Richtel, *supra* note 33 (asserting that the industry has begun to allow advertising on mobile phone menus, known in the industry as "on-deck" advertising). See generally Wayne R. Barnes, *Rethinking Spyware: Questioning the Propriety of Contractual Consent to Online Surveillance*, 39 U.C. DAVIS L. REV. 1545, 1552-53 (2006) (proposing definitions of spyware and adware that include "software ranging from 'keystroke loggers' that capture every key typed on a particular computer; to advertising applications that track users' web browsing; to programs that hijack users' system settings").

352. Cleff, *supra* note 349, at 267-68

353. *Id.*

354. *Id.*

policies covering m-advertising that are similar to those used with respect to obtaining consumer consent in other electronic or online contracts. These would include the possibility of obtaining implied consent based on presentation of browse wrap contracts to consumers that require consumers to take no action to signify agreement. Additionally, click-wrap contracts could be used to obtain more positive evidence of assent to the terms of a privacy policy for m-advertising as they require consumers to check a box signifying agreement with the terms or to uncheck an already checked box if they do not agree with the terms. Additionally, the consumer could signify his or her consent by making a mobile telephone call or sending a text message to the m-advertiser to convey agreement with the terms of a privacy policy. Further, disclosure of a privacy policy and obtaining consent to the terms of a privacy policy supporting m-advertising could be handled by the consumer's telecommunication carrier when the consumer subscribes to mobile phone service. For example, as part of service contracts for mobile phones that are typically signed by consumers at the time they obtain mobile phone service from their carriers, the carriers' subscription contracts could make the appropriate privacy disclosures and obtain consumers' consent to collection and use of their PII and their agreement to receive m-ads.

Such service agreements could be used to obtain consumer consent to receive otherwise unsolicited m-advertising, including the types of ads that the consumer is willing to receive, the form of those ads (e.g., whether text messages or voice calls), and perhaps the number and frequency of the ads that the consumer is willing to receive over a week, month, or year, etc. Since incoming voice and text messages often come at a cost to the consumer, contractual limitations on the scope of consent for unsolicited advertising are likely to be important to a consumer. For example, mobile subscribers often pay per-message fees for receiving or sending text messages or may pay for the receipt of m-advertising indirectly by having their available voice minutes reduced.<sup>355</sup> As consumers' contracts with their mobile carriers are form contracts drafted by the carriers, consumers are

---

355. For example, Cingular's service agreement charges the subscriber for incoming and outgoing text messages whether the text message is read or unread, solicited or unsolicited. Cingular Wireless Corp., Cingular Media Bundle Packages (2007) (on file with author). The senders' obligation under CANSPAM to give specific notice and to obtain express prior authorization from consumers before sending MSCMs takes into account the fact that mobile subscribers are generally incrementally charged for receiving unsolicited MSCMs in the form of voice, text or other messages on their cello phones. *See generally* Fed. Rules and Regs. Implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, *Order*, 19 F.C.C.R. 15927 p.9 (2004). Senders of MSCMs are required to give notices to consumers and to obtain their express prior authorization to send them MSCMs in a manner that does not result in any additional cost to the recipients. *Id.*; *see generally*, discussion of MSCMs at *supra*, Section V.B.

likely to be placed in a take it or leave it situation with respect to these contracts. Nevertheless, if the notice element of fair information practices is met through such contracts, and the contracts actually provide consumers with some choices as to use of their PII and whether or not they are willing to receive otherwise unsolicited m-advertising, mobile subscription agreements could be used to obtain consumers' consent.

## 2. The Use of Privacy Enhancing Technologies as an Alternative to Privacy Policies

At least theoretically, technological solutions designed to protect consumers' privacy in e-commerce could be used in m-commerce and m-advertising as an alternative to government regulation and to support industry self-regulation in the form of helping consumers evaluate m-advertisers' privacy policies and facilitate obtaining appropriate consent for the collection and use of PII and receipt of m-advertisements.<sup>356</sup> The term Privacy Enhancing Technologies ("PETs") encompasses "technical and organizational concepts" that aim to protect a consumer's identity and often involve encryption in the form of "digital signatures, blind signatures or digital pseudonyms."<sup>357</sup> Advantages of PETs are that they may offer those in mobile commerce anonymity and enable the consumer to participate without providing his or her PII.<sup>358</sup> A second potential technological solution, Platform for Privacy Preferences ("P3P"), has also been proposed as a potential technological solution to protect consumer privacy in e-commerce.<sup>359</sup> P3P is software designed to monitor Web site privacy policies. It enables consumers to communicate their privacy preferences before the Web sites that they visit are able to collect their PII and then consumers make choices about whether to visit the Web sites and, if so, to provide their PII.<sup>360</sup> P3P is underutilized at the present "due to a lack of significant customer and industry buy-in."<sup>361</sup> Although P3P was designed for traditional e-commerce, P3P could become an effective tool to help consumers exercise choices related to privacy policies associated with m-advertising, but first the technology would need to be made compatible with the mobile environment.<sup>362</sup>

---

356. SOLOVE ET AL., *supra* note 29, at 642-43.

357. *Id.* at 624 (internal quotations omitted).

358. *See id.*

359. *Id.* *See also* Ciocchetti, *supra* note 56, at 97.

360. Ciocchetti, *supra* note 56, at 97.

361. *Id.*

362. Cleff, *supra* note 349, at 267-68 (reporting on a project called Privacy in Mobile Internet (PIMI) that has the objective of developing an advising privacy platform for small displays like those found on mobile phones).

### *E. Why the Market Approach to Data Privacy Does Not Currently Ensure Appropriate Consumer Consent for M-Advertising*

Although company-specific and industry association privacy codes are an important component of protecting consumer privacy in m-commerce, as a general matter, industry self-regulation by itself has not resulted in effective consumer privacy protections absent supporting government regulation and enforcement.<sup>363</sup> So, to the extent that U.S. privacy laws do not adequately protect consumers' privacy in the mobile commerce and advertising context, this Article argues that regulatory reform is needed in the U.S. to protect consumers' privacy and personal data.<sup>364</sup> The next section focuses on fair information practices for m-advertising, particularly on whether or not existing federal regulation is adequate to ensure meaningful consumer consent for the use of consumers' PII for m-advertising purposes.

#### 1. Voice Calls Made to Mobile Phones

Currently, federal regulation allows m-advertisers to place voice calls to consumers to pitch products and services to them as long as the call is made by a live person and the call is not generated by autodialing. If the advertiser is calling a mobile phone number, the advertiser does not need to get the subscriber's consent in advance of making the call even if the advertiser is a telemarketer unless the consumer has listed their number on

---

363. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1680-82 (1999) (explaining that the market approach to privacy relies on "interactions between individuals and data processors to generate and maintain appropriate norms for information privacy," and concluding that a failure exists in the U.S. privacy market); see also Seventh ITU Internet Report, *supra* note 2, at 92 (arguing that "[t]o be effective, self-regulation requires an enforcement framework that facilitates communication between consumers and companies, from dispute resolution to consumer education and awareness," and a third party to verify and monitor enforcement); Ciocchetti, *supra* note 56, at 98 (arguing that gap between the theory of information privacy best practices and the actual nature of electronic privacy policies that are in place in U.S. companies today should be remedied through congressional action to enact a new federal information privacy law).

364. See generally Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection (Version 3.0)*, 2006 IL. L. REV. 357 (2006) (arguing that data privacy regulation is urgently needed in the U.S. to protect consumer privacy from abuses that may arise from unauthorized collection, storage, and sale of personal data, and proposing a model regulatory regime); see also Seventh ITU Internet Report, *supra* note 2, at 87-88 (summarizing the components of the Solove/Hoofnagle Model including proposals to address perceived data privacy problems in the U.S. such as: lack of consumer awareness of data privacy issues due to current anonymity of data brokers; the need for public disclosure of the data collection activities of companies; cumbersome opting-out processes; lack of control over who has access to personal information; and lack of accountability by companies when security or privacy breaches have occurred). However, currently no generally applicable privacy legislation exists in the U.S. See PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 1-3, 7-8 (1996).



the National Do Not Call Register or has made a company-specific do-not-call request to the advertiser. Even if consumers have registered their numbers on the National Do Not Call Register, m-advertisers with established business relationships may place live m-advertising calls to consumers on their mobile phones without obtaining advance consent as long as the consumers have not made company-specific do not call requests. Therefore, federal regulation does not currently protect consumers from being subjected to live m-advertising calls on their cell phones because it requires consumers to take the initiative to register their numbers on the National Do Not Call Register. Further, it can be expected that many advertisers will be outside the jurisdiction of U.S. laws or will ignore the National Do Not Call registration. One reason that more unsolicited m-advertising calls are not being received more frequently by consumers is that there are no official mobile phone number directories that make consumers' mobile phone numbers generally available. However, there is no federal law that precludes mobile carriers from disclosing consumers' mobile phone numbers for the creation of directories. Further, unofficial directories may be created by businesses formed to deliver m-ads, data banks, and m-advertisers.

There is also the potential that m-advertisers will use location data about consumers' mobile phones to target them with time- and location-specific advertisements through voice calls or text messages. However, to the extent that m-advertisers must obtain consumers' location data from mobile telecommunications carriers, the carrier is precluded from releasing this form of CPNI without consumers' advance authorization, at least to the extent that the disclosure of the location data is for marketing purposes by third parties that are unrelated to the mobile carrier.

## 2. Electronic Messages Sent to Mobile Phones

If an advertiser sends a text, multimedia or other form of electronic advertising message to a mobile phone and the advertiser does this without using a wireless Internet domain name on the FCC's official list, CAN-SPAM's "opt-out" notice and consent rules apply, meaning the advertiser does not need to obtain consent in advance. For example, a text message sent from the advertiser's phone to a cell phone ("phone to phone" text message) requires only "opt-out" notice, because it can be sent without using a wireless Internet domain name.

On the other hand, if the text message is covered by the MSCM rules, CAN-SPAM requires the advertiser to obtain the express authorization of the mobile phone subscriber in advance of sending the mobile advertisement, i.e., "opt-in" consent. For example, "txt.att.net" is currently

on the FCC's official list of wireless Internet domain names.<sup>365</sup> To send a text message to a consumer who is a subscriber of AT&T Wireless, the advertiser only needs to know the subscriber's mobile phone number and that she subscribes to AT&T mobile service. The advertiser can then address an email to the consumer using her mobile phone number and the "txt.att.net" domain name, as follows: "10digitmobilenumber@txt.att.net."<sup>366</sup> The m-ad can be sent to the consumer from any Internet email address, and it will be delivered to the consumer as a text message on her mobile phone.<sup>367</sup> The consumer will pay for receiving the m-ad as a text message under the consumer's subscription agreement with AT&T Wireless.<sup>368</sup> If the consumer has not purchased a plan from AT&T Wireless that includes text messages as part of her monthly subscription fee, the consumer will be charged an additional amount for receiving each text message.<sup>369</sup> Under AT&T's standard terms, text messages that are over 160 characters are split into multiple text messages and the consumer pays separately for each text message received.<sup>370</sup> If the text message has the primary purpose of advertising a product or service, the MSCM rules will apply, so prior to sending the MSCM, the sender must obtain the consumers' express authorization in written, oral, or electronic form. Click-wrap and other form contracts drafted by advertisers, mobile carriers, and other third parties conceivably may satisfy the advance authorization requirement to send MSCM advertising, although the advertiser is not allowed to send an MSCM message to consumers to obtain that consent and the notices required to send a MSCM must be separately stated. There is also a general exception to the requirement that mobile advertisers obtain advance authorization to send MSCMs, and this exception allows for the sending of transactional or relationship messages to mobile phones without the express authorization of mobile phone subscribers. To fit within this exception, the primary purpose of the electronic message sent directly to a consumer's mobile phone using a domain name on the FCC's official list must be to facilitate a business transaction or to provide warranty, product recall, safety, or security information to the consumer.

Since consumers generally have no privacy rights with respect to use or disclosure of their mobile phone numbers, there is a risk that m-spammers will ignore the MSCM rules requiring them to obtain prior

---

365. See discussion and notes, Section V.B.

366. See AT&T, What is the E-mail address for Text Messaging, etc.?, *supra* note 122.

367. *Id.*

368. *Id.*

369. *Id.*

370. *Id.*

express consent before sending m-ads directly to consumers' mobile phones, perhaps because the spammers are located outside the U.S. and don't fear FCC enforcement. Also, the MSCM rules will not protect consumers from receiving all forms of m-ads, because m-advertisers may legitimately use consumers' mobile phone numbers to send "phone to phone" text, multimedia and other messages, as long as they don't violate their own privacy policies or the Telemarketing Sales Rule. Although no mobile phone number directories are currently available that include official mobile phone numbers provided by mobile carriers, unless consumers employ blocking technology, their mobile phone numbers may, and will, be captured digitally by businesses that consumers call using their mobile phones. Once captured, consumers' mobile phone numbers may be stored in computerized databases and even made available over the Internet. Absent a privacy policy restricting collection, use, and even third-party disclosure of consumers' mobile phone numbers, there is no federal law that precludes businesses from creating databases of mobile phone numbers.

Voluntarily adopted privacy policies conceivably could provide privacy protections for consumers' PII including their mobile phone numbers. When an m-advertiser's policy restricts the collection, use, and disclosure of consumers' mobile phone numbers and the m-advertiser violates that policy, the primary legal risk is that the FTC will initiate an enforcement action against the m-advertiser for false and deceptive practices. Since the m-advertiser may minimize this risk by carefully drafting its privacy policy to disclose its plan to collect, use, and even disclose consumers' mobile phone numbers to avoid making promises that it cannot keep, this legal risk is a manageable one. The ease of avoiding liability under the FTC's rules also makes it unrealistic to depend on this form of industry self regulation to protect the privacy of mobile phone numbers and other forms of PII. Unless consumers' mobile phone numbers are given privacy protection under federal law, consumers are likely to receive mobile spam including unsolicited text message and multimedia advertisements. One solution would be to make it unlawful for businesses to collect, use, or disclose consumers' mobile phone numbers without their express authorization and to prohibit disclosures of consumers' mobile phone numbers to third parties.

### 3. Ads Displayed on Web Sites Accessed with Mobile Phones

Ads displayed on Web sites accessed with mobile phones do not present any special problems for consumers with one important exception: Consumers' mobile phone numbers may be digitally captured by the Web sites visited. Once the Web advertisers have collected consumers' mobile

phone numbers, the advertisers may then use them to generate future m-advertisements to consumers or may even sell or otherwise disclose consumers' mobile phone numbers to other advertisers or businesses.

Of course, consumers' cell phone numbers are just one form of PII collected by Web sites. Information about their Web surfing behavior, online purchases, payment details including credit card numbers, mailing addresses, and other such personal information are also routinely collected by Web sites. In m-commerce, the potential for m-advertisers to combine consumers' PII related to their purchasing behavior with consumers' mobile phone numbers creates heightened privacy concerns for consumers. Consumers' PII can be used to target them with more invasive forms of mobile advertising and subject them to greater risk of identity theft and other forms of fraud.

As discussed with respect to m-advertising delivered by voice and text messages to consumers' mobile phones, in order to protect consumers' privacy and personal data, it will be essential to consider the impact of m-advertising generated through websites visited by consumers' using their mobile phones and to require advertisers to give appropriate notice and obtain consumer consent for the collection, use, and further disclosure of consumers' mobile phone numbers and other PII. Federal legislation is likely needed to ensure this result.

#### 4. Ads Generated by Adware or Spyware Loaded on Cell Phone Handsets

The consumer privacy concerns associated with ad-generating software loaded on personal computers connected to the Internet may soon be extended to mobile phones as adware and spyware are loaded onto and stored on cell phone handsets. Adware on mobile phones will allow m-advertisers to generate m-advertising to consumers that will be displayed on consumers' mobile phone screens, and conceivably delivering m-ads by this method will not be subject to the MCMS rules of CAN-SPAM or involve autodialing restrictions imposed by the Telemarketing Sales Rule. Further, because the personal information that may be collected by adware and spyware for m-advertising purposes is not being processed by telecommunication carriers subject to CPNI rules, the primary source of federal data protection for telecommunications subscribers is also not applicable. M-ads delivered by adware may be location- and time-specific, perhaps triggered by passive RFID chips in the phones that are read by nearby RFID readers installed by advertisers in public places, such as shopping centers or entrances to stores in a shopping district. Adware or other software that is used to generate m-advertising may involve deceptive practices, and thus constitute spyware. For example, unwary consumers

may not know that adware software downloaded onto their mobile phones collects consumers' PII and transmits it to advertisers or other persons. To the extent that adware and spyware come with inadequate notice or are downloaded with inadequate consent, those who place such software on consumers' mobile phones may be the subject of FTC enforcement actions related to false and deceptive practices. The FTC has called on Congress to adopt legislation to regulate false and deceptive practices involving adware and spyware, as discussed earlier in this Article.<sup>371</sup> Any such legislation should address the potential that adware and spyware may be installed and operated on mobile phones and not just computers connected to the Internet.

#### *F. Proposal for Regulatory Reform to Ensure Appropriate Consumer Notice and Consent for M-Advertising*

This Article proposes several modest regulatory reforms designed to ensure the fair information practices of adequate notice and appropriate consumer consent for m-advertising.

##### 1. The Need to Protect the Confidentiality of Cell Phone Numbers

Federal legislation should be adopted to protect the privacy of consumers' cell phone numbers. The federal legislation should prohibit the disclosure to a third party of a consumer's mobile phone number without obtaining consent from the consumer on an "opt-in" basis. It should also prohibit publication of mobile phone directories and mobile phone marketing lists that include consumers' mobile phone numbers except on an "opt-in" consent basis. A Web search reveals numerous Web sites that provide directories of cell phone numbers for consumers and business subscribers for a fee.<sup>372</sup> Currently, none of these directories provide official information about cell phone numbers because the mobile operators do not

---

371. See CRS Report for Congress on Spyware, *supra* note 83.

372. See, e.g., CellPhoneNumbers.com, Cell Phone Numbers, <http://www.cellphonenumber.com/> (last visited Jan. 10, 2008) (reporting on the best cell phone directory sites including ReverseMobile.com, Reverse Phone Detective, PhoneNumberScan.com). Most of these directories provide the names of people who are associated with a telephone number (reverse cell phone directories). However, in January 2008, an online cell phone directory was launched by a company listing 90 million cell phone numbers of U.S. subscribers, made available for a fee, without first obtaining the consent of subscribers to include their numbers in the directory and reportedly making it very difficult for subscribers to "opt-out" of having their phone numbers made available through the site. See Alex Johnson, *Cell Phone Directory Rings Alarm Bells*, MSNBC.COM (Jan. 30, 2008), <http://www.msnbc.msn.com/id/22902400/>. After only a few days, the company discontinued this online directory of cell phone numbers, reportedly after receiving complaints from consumers and Verizon Wireless. See *Start-up Shuts Down Cell-Phone Directory After Consumer Complaints*, MERCURYNEWS.COM (Feb. 4, 2008), available at [http://www.mercurynews.com/ci\\_8165669?source=rss](http://www.mercurynews.com/ci_8165669?source=rss).

currently release subscribers' cell phone numbers for directory purposes.<sup>373</sup> Regulation to protect the privacy of consumers' cell phone numbers should give the consumer the right to withdraw his consent at any time. The regulation should set fair information practices for all persons or businesses that publish the mobile phone numbers of U.S. subscribers for any commercial purpose.

Further, the use of form contracts to obtain consumer consent to disclose their mobile phone numbers to a third party or to publish mobile phone numbers in a directory should be federally regulated. A short form disclosure should be required by federal law as part of the required process to obtain consent for a disclosure or publication of a consumer's mobile phone number. The required form should mandate the use of understandable wording that clearly conveys the consumer's right to refuse to give his consent. The person requesting a consumer's consent to disclose or publish a mobile phone number should be required to notify the consumer that access to goods or services may not be denied or conditioned on giving consent. Further, consumers' mobile phone numbers should be included in the definition of CPNI such that mobile carriers would not be permitted to disclose consumers' cell phone numbers to third parties for marketing purposes without obtaining consumers' authorization in advance ("opt-in" consent).

## 2. The Need for Meaningful Short Privacy Notices for Mobile Advertising

Short privacy notices that are capable of being displayed on mobile phones should be used in mobile advertising. A few of the essentials of using multilayered privacy policies is that even the short initial notice must be provided in a form that is compliant with relevant law, must communicate the information necessary to make informed decisions (including whether or not to proceed to use the Web site via the consumer's mobile phone given the terms of the site's privacy policy), and must avoid surprises by drawing attention to any processing that goes beyond established or expected norms. Since the key privacy risks associated with m-advertising concern both the collection, use, and disclosure of consumers' PII and the possibility that consumers will open themselves to receiving unsolicited advertising on their mobile phones, short form privacy notices that consumers encounter when visiting Web sites using their mobile phones should address these concerns.<sup>374</sup> For example, the

---

373. See *supra* Section V.D.2.

374. This Article is not the first to consider the design of privacy policy for display on mobile phones. For example, Corey Ciocchetti's analysis of privacy policies for e-commerce proposes a sample multilayered electronic policy suitable for display on mobile

following short notice could be used as part of a multilayered privacy policy by a business engaged in operating a mobile commerce Web site to notify consumers about the company's privacy practices:

**Figure 1**

**Sample Privacy Policy of a Company Engaged in Mobile Advertising**

**Privacy Policy of MOBILE-AD Company**

We collect personal information about you to market to you and to service your account. You may tell us not to do so.

We will not send advertisements to you on your cell phone without your consent.

We keep your cell phone number private and will not disclose it without your consent.

You may view our complete privacy policy at <http://www.MOBILE-AD> or call our service representative at [phone number] if you have questions.<sup>375</sup>

**3. The Need for Additional Protections Related to Consumer Location Data**

Companies that collect consumers' location data for the purpose of generating m-advertising solicitations to them should consider the consumer privacy interests associated with this practice. Currently, companies will not be able to get this data from mobile carriers unless the consumer has given her consent in advance. But will the carrier be able to send the consumer mobile advertising on behalf of third party advertisers without revealing CPNI like location data to the mobile advertiser? The carrier is in a unique position to generate revenue by conveying such ads to consumers on their mobile phones. Perhaps carriers will seek to give notice of their privacy practices and obtain consumer consent for the tracking of consumers' locations and receipt of mobile ads in subscription agreements for mobile services.

---

phones that is a significant contribution to this discussion. *See* references and text discussing Ciochetti's proposed model, *supra* note 333, at 101-03. The model "Privacy Policy for Mobile Advertising Company" proposed in this Article is made with recognition of the contributions of other scholars to the scholarship of model privacy policies, while aiming to advance the discussion by proposing sample wording for mobile privacy policies that will address the specific privacy concerns for consumers related to m-advertising.

<sup>375</sup> This proposed sample privacy policy is not designed for use by advertisers sending MSCMs, including text or multimedia ad messages that are sent directly to mobile devices using wireless Internet domain names on the FCC's official list. The "opt-in" notice and consent requirements for sending MSCMs require advertisers to convey additional information to consumers, limit the means of delivering the notice and specify minimum requirements for obtaining adequate consumer consent to constitute express authorization to send MSCMs. *See* discussion and notes, *supra* Section V.B.

Absent access to CPNI in the form of location data about consumers' mobile phones, an alternative is for mobile advertisers to use adware loaded on consumers' mobile phone handsets to deliver mobile advertisements. If mobile handsets come with the adware and are RFID-equipped, the m-advertiser would be in a good position to deliver location- and time-specific mobile ads. The handset manufacturer could load the adware on the mobile phone before delivering it to the consumer. In this case, consumer consent to receive such ads could be included in the contract between the retailer and the consumer, with the handset manufacturer, adware software designers, and m-advertisers being potential third parties to this contract. Privacy issues with this approach include delivering privacy notices and disclosures related to the adware and its capabilities, including consent to receive m-ads on the mobile phone, and obtaining appropriate consumer consent at the time the consumer purchases the mobile phone. The m-advertiser would install RFID readers in appropriate locations and be in a position to read the RFID tags in consumers' mobile phones when they are nearby in order to generate pop-up and other forms of advertising on consumers' mobile phones using the adware that is already installed.

Another way for m-ads to be delivered to consumers' mobile phones is for m-advertisers to download the adware to consumers' mobile phones when they visit a Web site using their mobile phones. If adware comes with adequate disclosures and the mobile phone user downloads the adware after those disclosures, consent to the adware and subsequent receipt of pop-up and other ads on the mobile phone would likely be implied from the fact that the consumer downloaded the adware. An end-user license agreement would likely accompany the download, and the consumer would be required to click on a box accepting the terms. If ad-generating software is deceptive or has malicious qualities associated with spyware, the FTC could find the privacy disclosures are inadequate or the users' consent invalid.

Because location-tracking privacy concerns with m-advertising are seriously invasive, federal regulation should set minimum standards for associated m-advertising practices. At a minimum, privacy disclosures should be required and there should be a requirement to obtain consumers' consent in advance of activating any adware or spyware that has been loaded on consumers' mobile phones. Consumers should have an easy and workable mechanism to remove any such adware or spyware, and false and deceptive practices should be prohibited. Finally, there should be a federal law that prohibits communicating location data about consumers' mobile phones to third parties without the consumers' express, advance consent.



### VIII. CONCLUSION

Consumers' mobile phones are the portal for mobile commerce—a convenient new form of doing business anywhere and anytime. Mobile advertising is an important component of this new business environment that is expected to fuel the growth of m-commerce. Mobile advertising raises a host of privacy and personal data protection issues for consumers that need to be analyzed within the context of existing government regulation and industry self regulation. These privacy and data protection concerns must be examined in light of the goal of allowing the mobile advertising industry to grow and prosper consistent with a business environment that promotes consumer trust and confidence.

As analyzed in this Article, a complex web of federal and state regulation exists that will govern mobile advertising. However, existing regulation is inadequate to protect consumers' privacy in mobile advertising. With a focus on providing adequate notice of privacy practices related to m-advertising and obtaining adequate consumer consent for m-advertising, this Article makes several simple suggestions for federal regulatory changes that include protecting consumers' mobile phone numbers as private data, providing meaningful short form privacy notices for use on mobile phone screens, and protecting location data about mobile phone users. Congress should adopt the regulatory reforms proposed in this Article because they are essential to protect consumers' privacy in this new mobile commercial context.