WHEN MOBILE PHONES ARE RFID-EQUIPPED—FINDING E.U.-U.S. SOLUTIONS TO PROTECT CONSUMER PRIVACY AND FACILITATE MOBILE COMMERCE

Nancy J. King[*]

Cite as: Nancy J. King, *When Mobile Phones Are RFID-Equipped—Finding E.U.-U.S. Solutions to Protect Consumer Privacy and Facilitate Mobile Commerce*
15 MICH. TELECOMM.TECH. L. REV. 107 (2008),
available at http://www.mttlr.org/volfifteen/king.pdf

New mobile phones have been designed to include delivery of mobile advertising and other useful location-based services, but have they also been designed to protect consumers' privacy? One of the key enabling technologies for these new types of phones and new mobile services is Radio Frequency Identification (RFID), a wireless communication technology that enables the unique identification of tagged objects. In the case of RFID-enabled mobile phones, the personal nature of the devices makes it very likely that, by locating a phone, businesses will also be able to locate its owner. Consumers are currently testing new RFID-enabled phones around the globe, but the phones are not yet in general use by consumers in the United States and Europe. The incorporation of RFID into cell phones in order to deliver mobile advertising and other location-based services raises a host of important privacy questions that urgently need to be addressed before the phones become widely available. Analyzing the risks to consumer privacy in this new context, this paper offers a comparative law analysis of the applicable

[*] Nancy J. King, J.D., M.S.T., Associate Professor, Oregon State University, College of Business, 200 Bexell Hall, Corvallis, Oregon 97331-2603, 541-737-3323, kingn@bus.oregonstate.edu. The author thanks the Fulbright Program and the Commission for Educational Exchange between the United States of America, Belgium and Luxembourg, European Union Affairs Program for the award of a 2007–2008 Fulbright Fellowship to support her research on privacy issues related to global regulation of mobile communications technologies. The author greatly appreciates her Belgian hosts at the Research Center in Informatics and Law (CRID), Facultés Universitaires Notre-Dame de la Paix, Namur, Belgium for offering insights on this research. This research also benefitted from insights gained through discussions about RFID and privacy-enhancing technologies with Professors Rene F. Reitsma and V.T. Raja from the College of Business, Oregon State University and legal and technical experts from CRID and the Université Catholique de Louvain, Louvain-la-Neuve, Belgium. Many thanks also to her husband, Brian King, an attorney with Schwabe Williamson & Wyatt in Portland, Oregon, for his careful review of drafts of this manuscript and suggestions for improvement which greatly contributed to its clarity and readability.

regulatory frameworks and recent policy developments in the European Union and the United States and concludes that there are many privacy concerns not presently addressed by E.U. and U.S. laws. This article also offers specific ideas to protect consumers' privacy through applications of fair information practices and privacy-enhancing technologies. When mobile phones are RFID-equipped, consumers will need new privacy protections in order to understand the risks and make knowledgeable decisions about their privacy.

Introduction

No longer simply mobile telephones, mobile phones can deliver new communication and information services for consumers that are made possible by location-aware technologies.[1] Location-based services (LBS)

1. Mobile phones come equipped with data, text and video streaming functions, making them much more than simple devices for making phone calls. Int'l Telecomms. Union [ITU], ITU Internet Reports 2005: The Internet of Things, 25–26 (7th ed. 2005), http://www.itu.int/osg/spu/publications/internetofthings [hereinafter *The Internet of Things*] (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). "[W]ith the development of mobile internet and mobile commerce service, users can buy theatre tickets, make hotel reservations, and access bank accounts through their mobile 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 companies in the telecommunications industry will shift their focus from providing voice communications to data transmission. *Id.* at 69.

A mobile (cell) phone is

for mobile phones empower subscribers to use their phones to find information about nearby businesses or services, such as movie theaters, banks or cafés.[2] They can also use their phones for navigation. For example, one user can receive directions from one location to another, locate another person's mobile phone, and receive updates or alerts about bus delays, traffic jams, or sales at nearby businesses. Mobile phones designed to receive location-based services will enable users to receive mobile advertising and other useful mobile services that are customized to them based on their geographic locations.[3] One of the enabling tech-

---

> [Actually a radio containing a low power transmitter. When a wireless telephone is turned on, it searches for a base station within range, which . . . 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.
>
> 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).

2. *See* K. Michael et al., *Location-Based Services and the Privacy-Security Dichotomy* (2006), http://ro.uow.edu.au/infopapers/382/ (published originally in PROCEEDINGS OF THE 3RD INTERNATIONAL CONFERENCE ON MOBILE COMPUTING AND UBIQUITUOUS NETWORKING 91–98 (London, Eng., Oct. 11–13, 2006)). "Location-based services (LBS) rely on knowledge of a user's location to provide tailored services or information by means of a wireless device . . . . Examples include . . . advertising targeted at a mobile phone that enters a particular cell . . . ." *Id.* at 2. *See also* Serena G. Stein, *Where Will Consumers Find Privacy Protection from RFID?: A Case for Federal Legislation*, 2007 DUKE L. & TECH. REV. 3 (2007) (discussing why U.S. laws are insufficient to address consumer privacy concerns related to the broad use of RFID technology in supply-chain and other contexts); Christoph Seidler, *RFID Opportunities for Mobile Telecommunication Services*, ITU-T TECH. WATCH (May 2005), http://www.itu.int/ITU-T/techwatch/rfid.pdf (defining RFID-based mobile telecommunications services as "services that provide information on objects equipped with an RFID tag over a telecommunication network."); Stefan Steiniger et al., Foundations of Location Based Services: Lesson 1, Lecture Notes on LBS, V. 1.0 (2006), http://www.geo.unizh.ch/publications/cartouche/lbs_lecturenotes_steinigeretal2006.pdf (providing non-exclusive categories of LBS applications including: navigation (e.g., car park guidance), information (e.g., travel guides), tracking (e.g., people, vehicles and products), games (e.g., mobile games), emergency assistance (e.g., automotive assistance), advertising (e.g., banners, advertising alerts), billing (e.g., road tolls), management (e.g., fleet scheduling), and leisure (e.g., buddy finder, instant messaging)).

3. Laura M. Holson, *In CBS Test, Mobile Ads Find Users*, N.Y. TIMES, Feb. 6, 2008 (reporting on CBS' plans to try a serious experiment with cell phone advertising that is customized for a person's location; participants must have GPS enabled phones and are required to "opt-in" to receive the ads); *see also* Marguerite Reardon, *Is Mobile Really a Sure Thing for Google?*, CNET NEWS, Feb. 8, 2008, http://news.cnet.com/Is-mobile-really-a-sure-thing-for-Google/2100-1039_3-6229619.html (reporting that Gartner, a research firm, shows that mobile advertising will grow from $1 billion in 2007 to $11 billion by 2011 and discussing barriers to Google's efforts to enter this market). *But see* Caroline McCarthy, *The Mobile Social: Not Ready for Prime Time?*, CNET NEWS, Feb. 13, 2008, http://news.cnet.com/8301-13577_3-9870611-36.html (describing how mobile phone technology and service currently limits the potential for businesses to provide mobile location-based services in the United

nologies for new location-based services is Radio Frequency Identification (RFID), which is "a wireless communication technology that is used to uniquely identify tagged objects or people."[4] In this case, the "tag" is a small computer chip with its own antenna that is attached to or embedded in a consumer product. It is designed to store digital information such as a unique number to identify an individual consumer product. For example, it can be used to distinguish one can of soda from another, even though the products are identical in all other respects.[5] The tag's antenna is able to broadcast that number and does not need to have its own power source because it operates by using energy received from nearby radio frequency identification readers that scan the tag.[6] Tags can be read by readers even when they are not in the line of sight of the reader and without human intervention.[7]

States, such as mobile phones that cannot process "geotagging" or "proximity alerts," and the prevalence of subscribers without data plans or plans that provide unlimited text messaging).

4. For an overview of RFID technologies and particularly the location tracking capabilities of RFID systems, *see* DANIEL HUNT ET AL., RFID: A GUIDE TO RADIO FREQUENCY IDENTIFICATION 1 (2007). For convenience, Radio Frequency Identification may be referred to as RFID in this paper. *See also* MARY RUNDLE & CHRIS CONLEY, ETHICAL IMPLICATIONS OF EMERGING TECHNOLOGIES: A SURVEY 41–50 (UNESCO, Commc'n and Info. Sector, 2007), http://unesdoc.unesco.org/images/0014/001499/149992E.pdf [hereinafter ETHICAL IMPLICATIONS OF EMERGING TECHNOLOGIES] (defining RFID and describing uses of RFID to track the location of people); Jonathan Weinberg, *RFID, Privacy and Regulation, in* RFID APPLICATIONS, SECURITY AND PRIVACY 91 (Simson Garfinkel & Beth Rosenberg, eds., Addison-Wesley Professional 2005) (describing the location tracking capabilities of RFID for consumer goods that are sold directly to individuals). Bluetooth is another technology that could be used to deliver advertising to cell phone users (e.g., via text message to the cell phone user) and raises similar privacy and security risks to the cell phone user. *Id.* at 303.

5. Stephen A. Weis, *RFID (Radio-Frequency Identification)*, *in* 3 HANDBOOK OF COMPUTER NETWORKS: DISTRIBUTED NETWORKS, NETWORK PLANNING, CONTROL, MANAGEMENT, AND NEW TRENDS AND APPLICATIONS 974, 976–77 (Hossein Bidgoli ed., Wiley, 2007).

6. *Id.*

7. *Id.* at 975. Currently, passive tags can be read from as far away as 30 feet and active tags can be read from an even greater distance, up to 300 feet. Katherine Albrecht, *RFID Tag—You're It*, SCI. AM., Sept. 2008, at 72, 75; Letter from Melissa Ngo, Senior Counsel, Elec. Privacy Info. Ctr., to Robert E. Clegg, Jr., Senator, N.H. 2 (Apr. 14, 2008), http://epic.org/privacy/rfid/epic_clegg_hb686.pdf [hereinafter EPIC Letter] (EPIC Analysis of H.B. 686). *See also* Beth Bacheldor, *Visa Partners with Nokia to Offer RFID-Enabled Services*, RFID J., Oct. 3, 2008, http://www.rfidjournal.com/article/view/4359/ (reporting that "Visa and mobile device manufacturer Nokia are joining forces to deliver new services, including contactless payments, money transfers and remote payments, on Nokia's newest . . . [NFC]-enabled handset."). "The NFC-enabled handset contains an RFID module that can function as an RFID tag and as an RFID reader," operates at 13.56 MHz frequency, supports ISO/IEC 14443, and will be available worldwide. *Id.* Nokia's new phone adds a feature of peer-to-peer communication "so that two NFC-enabled handsets can communicate and exchange information with each other by tapping them together (or bringing them within 4 centimeters of one another)." *Id.* ISO 14443 is an industry standard that "was developed specifically for identification and payment cards and has a degree of security and privacy protection built in." Albrecht, *supra*, at 74. "In contrast, U.S. border cards use an RFID

Radio frequency identification technology is likely to be incorporated into mobile phones in the near future. In several parts of the world, consumers are already testing mobile phones equipped with radio frequency identification devices and experience the ease of making payments for things like transit fares and fast food purchases.[8] They are also getting a first taste of mobile advertising on their RFID-enabled mobile phones because the phones come equipped with RFID-readers. The reader can be used to scan advertising and other information from nearby RFID tagged items in consumers' environments, such as "smart" advertising posters placed in transit terminals to obtain information about nearby restaurants or promotional materials about new products and services.[9]

The advent of location-based services, including mobile advertising, and the incorporation of RFID into cell phones for the purpose of delivering these services raises a host of important privacy questions that urgently need to be addressed while there is still time to protect consumers' privacy through privacy-enhancing design decisions and/or legislative action.[10] The privacy issues relating to the provision of location-based services and mobile advertising include the need to protect location and other personal data that is collected and used.[11] Other pri-

---

standard known as EPCglobal Gen 2, a technology that was designed to track products in warehouses, where the goal is not security but maximum ease of readability." *Id.* "[T]he ISO 14443 standard includes rudimentary encryption and requires [contactless payment] tags to be close to a scanner to be read," generally "a distance measured in inches rather than feet." *Id.* Of course, a mobile phone could contain more than one RFID tag, which could be used for different purposes (e.g., identification of device for repair services, or facilitation of contactless payments), and those tags could have different read ranges.

8. Recent consumer trials of RFID-enabled mobile phones in RFID-embedded public spaces are discussed in Part III, *infra*.

9. *Id.*

10. For a definition of location-based services (LBS), see discussion and references, *supra* note 2. *See also* D. Zachary Hostetter, *When Small Technology Is a Big Deal: Legal Issues Arising from Business Use of RFID*, 2 SHIDLER J.L. COM. & TECH. 10, ¶¶ 10–13, 23–28 (2005) (article paginated by paragraph number); *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, 308–10 (2004) [hereinafter *Recent Development in Harvard Journal of Law & Technology*] (discussing location privacy concerns in the context of law enforcement use of cellular location information). *See also* Murray Long, *Longitude and Latitude: Location Technologies and Privacy Concerns*, 29TH INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS, Montreal, Canada, at 9–11 (Sept. 26, 2007) http://www.privacyconference2007.gc.ca/workbooks/Terra_Incognita_workbook4_E.html#section002. Long discusses the tracking potential of RFID systems and Professor Wienberg's suggestion that information sharing among operators of discrete reader networks could create a massive shared network which becomes a "Panopticon geolocator." *Id.* (citing Weinberg *supra*, note 4, at 91).

11. *See Working Party 29 Opinion on the Use of Location Data with a View to Providing Value-Added Services*, 2130/05/EN, WP 115 (Nov. 2005), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf [hereinafter *Working Party Opin-*

vacy concerns relate to the possibility of exposing consumers to more spam and the enhanced risk of unauthorized persons gaining access to personal information stored on mobile phones.[12] Privacy questions also arise from RFID applications that enable marketers to automatically track and profile consumers in order to deliver time and location-specific advertising to them on their mobile phones.[13] These privacy and data protection concerns are grounded in emerging scholarship about the vision of an ambient intelligence (AmI) era[14] that includes discussion of the

---

ion on Location Data]. This opinion discusses application of the European Union's data protection laws to the processing of personal data by entities that provide location-based services (LBS) to users and subscribers. *Id.* at 2. It recognizes several possible sources of location information about individual persons that may be used to provide location-based services, which include: processing data from satellites (GPS), processing data from an electronic communications network (e.g., mobile phone communications network or Wi-Fi network), or processing data from any other device, such as an RFID tag located by a reader. *Id.* at 10.

12. *See* Kim Hart, *Advertising Sent to Cellphones Opens New Front in War on Spam*, WASHINGTONPOST.COM, Mar. 10, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/03/09/AR2008030902213.html (reporting that a market research study shows U.S. consumers are expected to receive about 1.5 billion spam text messages in 2007); Bob Sullivan, *Hit by ID Theft, Then Plagued by Sprint?*, THE RED TAPE CHRONICLES—MSNBC.COM, Mar. 7, 2008, http://redtape.msnbc.com/2008/03/you-might-call.html (reporting the travails of a cell phone customer hit by an ID thief who added fourteen new lines to his account and extended his terms of service agreement, resulting in additional charges of over five thousand dollars and an early termination fee).

13. *See generally* SERGE GUTWIRTH, PRIVACY AND THE INFORMATION AGE 49–60, 83–108 (Rowman & Littlefield Pub. 2002) (discussing the concept of privacy, focusing on the concept of the individual's freedom to be oneself, and how this concept is related to the rights of individuals with respect to the processing of personal data in this information age characterized by pervasive computing). *See also* Jean-Marc Dinant et al., *Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data: Application of Convention 108 to the Profiling Mechanism—Some Ideas for the Future Work of the Consultative Committee*, CENTRE DE RECHERCHES INFORMATIQUE ET DROIT (CRID), (Jan. 2008), http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/T-PD(2008)01_en_profiling.pdf.

14. *See* Antionette Rouvroy, *Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence*, 2-1, art. 3 STUD. IN ETHICS, L. & TECH. 1–5 (2008) (stating the "two aspects—freedom from unreasonable constraints (from the state or from others) on the construction of one's identity, and control over (some) aspects of the identity one projects to the world—are at the heart of the most crucial concerns arising when considering, from a legal and political point-of-view, the emerging AmI *scenarios*." (emphasis in original)); *see also* TECHNOLOGY AND PRIVACY, THE NEW LANDSCAPE 7 (Philip E. Agre & Marc Rotenberg eds., MIT Press 1998) (explaining the relationship between data protection and privacy as: "Control over personal information is control over an aspect of the identity one projects to the world, and the right to privacy is the freedom from unreasonable constraints on the construction of one's own identity."). Rouvroy further explains:

> Those two aspects—freedom from unreasonable constraints (from the state or from others) on the construction of one's identity, and control over (some) aspects of the identity one projects to the world—are the heart of the most crucial concerns arising when considering, from a legal and political point-of-view, the emerging AmI scenarios.

Internet of Things, the dissemination of RFIDs, ubiquitous computing, smart objects and surveillance devices.[15]

The primary goal of this Article is to convey the results of a comparative law study of E.U. and U.S. regulatory efforts to address the privacy and data protection implications of consumer marketing practices that employ RFID technologies for the purpose of delivering mobile advertising and other location-based services. Ultimately this article strives to answer the question: When mobile phones are equipped with RFID to support delivery of location-based services and mobile advertising, what consumer privacy protection is needed to ensure the level of consumer trust necessary for the growth of mobile commerce and how best to achieve it?

The article identifies five important privacy and data protection issues for consumers in this new business context that features RFID systems that operate invisibly and automatically in the background.[16] It examines the regulatory frameworks and existing government regulation in both the European Union and the United States that form the foundation for the regulation of RFID-enabled mobile phones used to deliver LBS and mobile advertising. Although more extensive government regulation is found in the European Union than in the United States, the study reveals similarities in E.U. and U.S. law. However there are also privacy gaps in the sense that important privacy and data protection concerns are not regulated under the current laws of one or both systems. Anticipating that LBS and accompanying mobile advertising will produce social, consumer, and commercial benefits,[17] and recognizing the relationship between consumer trust and adequate protection of consum-

---

Rouvroy, *supra*, at 7.

15. *See generally The Internet of Things*, *supra* note 1, at 25–26 (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).

16. Org. for Econ. Cooperation & Dev. [OECD], Working Party on Info. Security & Privacy, *Report, Radio Frequency Identification (RFID): A Focus on Information Security and Privacy*, DSTI/ICCP/REG(2007)9/FINAL, 5 (2007), *available at* http://www.olis.oecd.org/olis/2007doc.nsf/linkto/dsti-iccp-reg(2007)9-final [hereinafter *OECD Report on RFID*] (commenting that the "invisibility of the data collection may be the primary characteristic of RFID that raises (privacy) concerns" and that "tracking in real time or after the fact may be the primary functionality of RFID that raises concerns").

17. Location data can provide value-added services to individuals based on knowing where their mobile phones are at a particular time (providing information upon request to a mobile phone user about the nearest restaurants, for example). *Working Party Opinion on Location Data*, *supra* note 11, at 2–3. Other location-based services enable individuals to be located via their mobile phones even if they have not requested the services. *Id.* at 3. Emerging technologies such as RFID have the potential to produce good as well as ill for society. *See generally* ADAM GREENFIELD, EVERYWARE 1–5 (New Riders 2006); ETHICAL IMPLICATIONS OF EMERGING TECHNOLOGIES, *supra* note 4, at 8–10.

ers' privacy and personal data,[18] the article concludes that these privacy gaps need to be addressed. It considers mechanisms to fill these voids using government regulation and/or industry self-regulation. After examining recent legal developments in the European Union and the United States that may close these gaps, this article discusses self-regulatory approaches that could be adopted by companies, such as implementing effective privacy policies and practices or designing RFID-applications using privacy-enhancing technologies. Further, recognizing the global nature of m-commerce,[19] where suppliers of LBS and mobile advertisers will communicate with mobile phone users across national borders and consumers' personal data will be easily transmitted to any place in the world via the Internet,[20] this study suggests that adoption of self-regulatory tools is the preferred method to protect consumers. The study concludes that the mechanism of privacy impact assessments and adoption of privacy-enhancing practices, coupled with regulatory oversight, is the most feasible approach to protect consumers' privacy in this emerging area of commerce.

---

18. Alfred Villoch III, Comment, *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, 446–48 (2002).

19. Mobile commerce (m-commerce or mobile e-commerce) is gradually emerging as a new global commercial environment due to the growing number of consumers who have mobile phones and other portable wireless electronic communications devices. *See* Peter Tarasewich et al., *Issues in Mobile E-commerce*, 8 COMM. FOR 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."). *See also* Sridhar Balasubramanian et al., *Exploring the Implications of M-Commerce for Markets and Marketing*, 30 J. ACAD. OF MARKETING SCI. 348–61 (2002) (providing a five component conceptualization of m-commerce that is separate from the underlying technologies related to mobile communications devices). Mobile commerce encompasses a wide range of interactive business processes that occur before, during and after actual sales transactions. *See* Tarasewich et al., *supra*, at 42. An important technological development that facilitates m-commerce and allows users to interact with information and services immediately by accessing the Internet through their mobile phones is known as wireless application protocol (WAP). Essentially, with WAP, consumers' mobile phones act as mini-Web browsers. Villoch III, *supra* note 18, at 447. Another important technological development for m-commerce is emerging RFID technologies that will enable mobile phone users with RFID-equipped mobile phones to purchase goods and services through "contactless" transactions between their phones and RFID systems embedded in the environment. *See infra* Part III.

20. *See Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on "Radio Frequency Identification (RFID) in Europe: Steps Towards a Policy Framework"*, COM (2007) 96, 2008 O.J. (C 101) 01, ¶ 15, *available at* http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_EN.pdf [hereinafter EPDS Opinion on RFID].

This Article offers input for the privacy impact assessments that will be the basis of designing privacy strategies, privacy policies and privacy-enhancing technologies to protect consumers from privacy risks related to RFID-enabled mobile phones. It provides three examples of the categories of privacy topics and related analyses to consider in privacy impact assessments for RFID-enabled mobile phones. The first category addresses application of essential fair information practices, such as providing adequate consumer notice regarding the privacy-implicating features of RFID-enabled phones. A second category relates to the need to explore the selection of privacy-enhancing technologies that could give consumers the ability to remain anonymous in some situations and perhaps even disable the RFID tags included in their mobile phones. A final category examines whether mobile phones should be designed to include transparency-enhancing features in order to make the privacy implications of using RFID applications more obvious to consumers, e.g., giving consumers access to personal information and classifications that are being collected by virtue of using RFID-enabled mobile phones and that will be used by marketers to target them for mobile advertising.

Finally, this article offers a list of RFID-specific privacy questions and possible technical solutions that relate to this new business context.[21] Discussions with technical experts on RFID and a review of the RFID-literature both support the conclusion that, at least theoretically, there are technical solutions for many of the perceived privacy concerns related to RFID-enabled mobile phones. The list is offered to stimulate discussion between technical and legal privacy experts who hopefully will work together to find privacy-enhancing solutions to adequately protect consumers' privacy in the era of RFID-enabled mobile phones, location-based services and mobile advertising. To the extent that such solutions are found, it will reduce the need for RFID-specific government regulation that could discourage further development of new and useful location-based services using RFID technologies and create legal barriers to global mobile commerce.

I. The Important Role Mobile Advertising May Play in Providing Location-Based Services for Consumers

Mobile advertising (m-advertising) is advertising directed at consumers through their mobile phones and it is likely to play an important role in business models to deliver LBS to consumers.[22] M-advertising

21. *See infra* Part VIII.

22. Eric Pfanner, *Mobile Phones Are a New Frontier in Advertising*, Int'l Herald Trib., Mar. 11, 2007 (on file with author) (reporting that approximately one billion mobile

refers to ads sent to and displayed on mobile phones and other handheld wireless communications devices.[23] As used in this article, m-advertising includes direct marketing as well as other forms of advertising that users may access on their mobile phones.[24] Like location-based services in mobile commerce, mobile advertising may be tailored to individual consumers based on their geographic location at a specific time.[25] In this respect, mobile advertising has advantages over print or broadcast advertising because it allows marketers to send location and time-specific, personalized advertisements directly to consumers.[26] Further, as

---

phones will be sold in the world in 2007); John Finegold, *How Your Wireless Network Will Change Your Social Network,* PEN COMPUTING, http://pencomputing.com/features/ulocate_lbs.html (last visited Jan. 4, 2009).

23. JAANA TÄHTINEN & JARI SALO, SPECIAL FEATURES OF MOBILE ADVERTISING AND THEIR UTILIZATION, PROCEEDINGS OF THE 33RD EMAC CONFERENCE 7 (EMAC, Murcia, Spain 2004), 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 reveals 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 2004, 590–605, http://www.ebrc.info/kuvat/590-605_04.pdf. Successful business models for generating revenues from mobile advertising are still being developed. *Id.* at 591. The business actors that are involved in creating value through mobile advertising include: (1) 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.

24. For a discussion of the distinction between advertising, including online advertising, and direct marketing, see E-COMMERCE LAW, DOING BUSINESS ONLINE 119–36 (Simmons & Simmons, Palladian Law Publ'g Ltd. 2001) (providing an overview of the regulation of online advertising and direct marketing in the United Kingdom). Generally, online advertising uses non-broadcast media and the content is available for viewing on a one-to-many basis. *Id.* at 119–21. However, transmission of that content does not happen simultaneously, but rather occurs when the Web site is accessed by each individual user. *Id.* Direct marketing is a business practice that involves communicating promotions of businesses' products and services directly to individuals, whether by telephone, fax, e-mail or other methods. *Id.* Direct marketing generally involves processing personal data about consumers. *Id.*

25. Of course, not all m-advertising is location or time-specific. For example, banner ads to be displayed on mobile phones need not be tailored to consumers' geographic locations at specific times, although the relevance of the ads to consumers could be enhanced if the ads were so tailored.

26. *See* James C. White, People, Not Places: A Policy Framework for Analyzing Location Privacy Issues (Spring 2003) (unpublished Masters Memo Prepared for the Electronic Privacy Information Center, Duke University), http://www.epic.org/privacy/location/jwhitelocationprivacy.pdf. M-Commerce businesses may use location information about consumers to create content "whose value comes from knowledge of where a user physically is," such as alerts about traffic jams or weather information. *Id.* at ii. *See also* Jari Salo & Janna

compared to online advertising directed generally to consumers using computers with Internet access, the prevalence of mobile phones among consumers and the personal nature of the devices, including the likelihood that consumers will have their mobile phones with them most of the time, make mobile advertising an attractive medium.

Advertisers, mobile telecommunications carriers (mobile carriers), mobile phone manufacturers (handset manufacturers) and other third parties (such as mobile service application providers) may all be involved in generating or delivering m-advertisements.[27] There are multiple forms of m-advertising. For example, advertisers may communicate their messages to consumers' mobile phones by calling mobile phone numbers to talk with consumers or sending voice, text, instant or multimedia messages (e.g., video clips) to consumers' mobile phone numbers.[28] It is also technically possible to send an electronic ad message directly to a consumer's mobile phone by sending it to a wireless Internet domain name provided by the consumer's wireless carrier.[29] Advertisements may also be displayed on mobile phones when consumers access Web sites using their internet access-equipped mobile phones.[30] Adware software programs loaded directly on consumers' phones by handset manufacturers or downloaded to consumers' cell phones from the Internet are another way to deliver mobile advertising.[31] This paper discusses yet an-

---

Tähtinen, *Retailer Use of Permission-Based Mobile Advertising*, *in* ADVANCES IN ELECTRONIC MARKETING ch. VIII (Irvine Clarke III and Teresa B. Flatherty, eds.) (2005); *Working Party Opinion on Location Data*, *supra* note 11, at 2–3.

27. Nancy J. King, *Direct Marketing, Mobile Phones and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices*, 60–2 FED. COMM. L.J. 239, 243 (2008).

28. *Id.*

29. *Id.* at 261–64. *See also* 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, 866–67 (2005).

30. *See, e.g.*, Matt Richtel, *Verizon to Allow Ads on Its Mobile Phones*, N.Y. TIMES, Dec. 26, 2006, at C5; Bob Keefe, *Cell Phones Poised to Become One More Ad-Driven Medium*, COX NEWS SERVICE, Sept. 12, 2006 (on file with author); Eric Sylvers, *Cell Phone Ads May Take Off Soon*, N.Y. TIMES, Feb. 14, 2007, http://nytimes.com/2007/02/14/business/media/14adco.html (reporting that Yahoo began displaying ads in early 2007 on sites accessible to subscribers with advanced cell phones in 19 countries). Mobile phone users would see the ads when going to Yahoo's home Web page on their phones and could then click on an ad to dial a company directly or to get more information and special offers). *Id.* Sylvers 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.

31. *See* Daniel B. Garrie & Rebecca Wong, *Spyware Technologies: Limiting the Horizons of Digital Privacy*, 23 T.M. COOLEY L. REV. 473, 479–81 (2006) (discussing adware that places random or targeted ads on the screen of the user and its relation to spyware, which is

other way to generate mobile advertising—building RFID technologies into mobile phone handsets and embedding RFID technologies into consumers' environments (like shopping malls or bus stations) for the specific purpose of delivering mobile advertising (and location-based services).[32] When the available methods of delivering mobile advertising are considered in conjunction with technological advances enabling advertisers to target advertising to individual consumers based on the geographic location of their mobile phones at a particular time, the enormous potential of the mobile advertising market is apparent. Not so obvious are the consumer privacy and data protection implications of using location tracking technologies to generate m-advertising, including the risk that mobile phones will become the new portal for spammers.[33] If left unregulated, mobile advertising and location tracking technologies may develop in ways that are simply too privacy-intrusive to support the healthy growth of global m-commerce.[34]

New social networking applications for Internet-enabled mobile phones provide location-based services that help people connect with friends and the places around them. They are a good example of new LBS services that have the potential to both benefit consumers and provide opportunities for businesses supplying the LBS services to generate revenues through location-based m-advertising.[35] Some of these new social networking applications are currently offered without charge to users, but create potential advertising revenue opportunities for suppliers, should they choose to convey mobile advertising to users along with social networking services. For example, one social networking

---

generally an application installed on a user's computer without their knowledge that can monitor everything that users do with their computers including their activities on the Web and transmit that information to an outside entity). New forms of these technologies may accompany e-mail messages, software programs or cell-phone applications (so-called "parisiteware" or "privacy-evading technologies"). *Id.* at 481.

32. *See* Parts III, IV.

33. *See* Laura M. Holson, *Spam Plague Is Migrating from Computers to Cellphones*, N.Y. TIMES, May 10, 2008, at C1 (reporting that cell phone spam is increasing and that most cell phone spam reaches cell phones through gateways that link the Internet and cell phones, such that a spammer may send e-mail that appears as text messages on cell phones by utilizing Internet addresses dedicated to wireless phones. At AT&T, for example, the address to send an Internet-to-phone electronic message is the customer's cell phone number followed by @text.att.net).

34. *See also* Laurie Thomas Lee, *Can Police Track Your Wireless Calls? Location Information and Privacy Law*, 21 CARDOZO ARTS & ENT. L.J. 381, 381–82 (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 [and commercial] use).

35. *See, e.g.*, Welcome to BuddyFinder, http://buddyfinder.com.au/buddyfinder.htm (last visited Jan. 4, 2009).

service enables members to locate their friends through their mobile phones.[36] To participate, members share their mobile phone numbers and the mobile phone numbers of friends that they would like to be able to locate with the social networking provider.[37] Scholars envision a privacy-enhanced model location-based mobile advertising platform (LAMM) for a social networking application that will enable mobile phone users to find and communicate with their friends. LAMM is designed to be able to deliver mobile messaging services along with mobile advertising while also incorporating design features to protect the privacy and personal data of users and to give users control over the time, frequency and types of mobile advertising messages they are willing to receive.[38] Designed to be compliant with data protection and spam laws in the European Union, one of the key features of LAMM is that it follows the principle of "opt-in" notice and consent; users receive a full privacy policy and give their explicit consent to have their locations tracked and to receive m-advertising messages.[39] Although the LAMM model employs different tracking technologies than the RFID applications discussed in this article,[40] it provides insightful analysis of the fundamental privacy and data protection issues involved in delivering LBS and m-advertising and is a useful starting point for considering the implications of delivering LBS and m-advertising using RFID-enabled phones in RFID-embedded environments.

In the future, mobile advertising may make it possible for consumers to receive free or reduced-cost mobile telecommunications services (e.g., voice, text, mobile Web access and LBS) in a system where the cost is offset by mobile advertising revenues, as opposed to the current user-

---

36. *Id.*

37. *See, e.g.*, Tour, BuddyFinder Tour™, http://buddyfinder.com.au/buddy-finder/tour.html (last visited Jan. 4, 2009).

38. *See* Evelyne Cleff & Gyozo Gidofalvi, *Legal Aspects of a Location-Based Mobile Advertising Platform*, 2 INT'L. J. INTELL. PROP. MGMT. 261 (2008). According to Cleff and Gidofalvi, their model (which they have named LAMM):

> LAMM is an effective vehicle for location-based [mobile] advertising [that] will create significant commercial opportunities. LAMM will provide the opportunity for users to check for the instant availability of people, communicate instantly and use the platform to exchange ideas and information. Messages in LAMM are, unlike Short Messaging Services (SMSs), not limited in length and are transmitted in real time. Moreover, LAMM enables users to indicate their status (available, busy, etc.), allowing for a context-sensitive and real-time communication channel. The same feature also enables control of the time and frequency of received advertising messages. Finally, messaging by means of LAMM will be more cost efficient than SMS.

Id. at 262. LAMM is a theoretical model not yet commercialized. *Id.*

39. *Id.* at 268.

40. *See id.* at 265.

paid subscription and fee model.[41] Perhaps mobile advertising will support free or lower cost telecommunications and information services for mobile phone users that are analogous to the role advertising revenues play in supporting online content. When contemplating the emerging context of location-based services and mobile advertising, it is essential to discuss the related consumer privacy and data issues. We need to do this now, while there is still time to ensure that consumer privacy and data protection concerns are given appropriate weight in the evaluation of technical design features, commercial feasibility and consumer benefit. This paper argues that the incorporation of RFID technologies into mobile phones, making it possible for advertisers to directly deliver targeted, location-specific advertising to consumers on their mobile phones, creates significant threats to consumer privacy and data protection that outpace the regulatory systems currently in place to protect consumers.

II. TECHNOLOGIES THAT SUPPORT LBS AND DELIVERY OF M-ADVERTISING

It is presently possible to electronically track the geographic locations, Web-surfing and other behaviors of mobile phone users who are using their mobile phones.[42] There are three technologies that work in conjunction with mobile phones to generate location data that could be used to enable businesses to identify mobile phone users' geographic locations in order to provide location-based services and

41. *See, e.g.*, Elinor Mills, *In Search of the Google Phone*, CNET NEWS, Oct. 24, 2007, http://news.cnet.com/In-search-of-the-Google-phone/2100-1041_3-6214939.html (speculating that the Gphone would be supported by advertising, based on filing of a patent application by Google for advertising-supported telephony); Amol Sharma, *Can a Google Phone Connect with Carriers?*, 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 some mobile devices" and "[i]f Google isn't careful, sensitive user information could end up in the wrong hands, leading to spamming, stalking and other invasions of privacy.").

42. However, currently the tracking technology may be unreliable in some situations. *See* John Dunbar, *Cell Phones Lack Reliable Area Tracking for 911 Emergencies*, CORVALLIS GAZETTE-TIMES, Apr. 25, 2007, at A7. 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 95 percent of the time and also requires companies that use handset technology (global positioning satellite (GPS) technology to locate callers) to come within 150 meters 95 percent of the time. *Id.* 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 United States, showed that the companies were unable to meet these standards a significant portion of the time. *Id.*

location-specific advertising.[43] First, the mobile phone user's cell phone number[44] and a unique Mobile Identification Number[45] (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 her mobile phone.[46] Second, location-tracking technologies utilizing Global

43. *See Recent Development in Harvard Journal of Law & Technology*, *supra* note 10, at 307–11 (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, including discussion of GPS and cell phone triangulation technologies); *Working Party Opinion on Location Data*, *supra* note 11, at 10 (discussing systems that produce location data based on information processed from GPS systems, telephone networks, or RFID tags located by readers, and the potential to identify individuals' locations through systems using these technologies by locating objects in their possession, such as mobile telephones).

44. *Recent Development in Harvard Journal of Law & Technology*, *supra* note 10, at 309 (the unique Mobile Identification Number enables carriers to use GPS or other tracking technologies to track a specific cell phone because it distinguishes an individual cell phone from all other cell phones).

45. *Id.* In the United States, the Federal Communications Commission (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 307. So, for example, there is no law that requires cell phones sold in the United States to have GPS chips.

46. 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 carry signals from the user's phone. Timothy Joseph Duva, Comment, *You Get What You Pay for . . . and so Does the Government: How Law Enforcement Can Use Your Personal Property to Track Your Movements*, 6 N.C. J.L. & TECH. 165, 169 (2004). Signal triangulation works in the following way:

> 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 to 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 the 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 a 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 service 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.

Positioning Service (GPS) technologies also enable mobile phone carriers to locate and track individual mobile phones.[47] Mobile phones equipped with GPS technology allow mobile communication networks to give the exact geographic position of mobile phones which are so equipped, and thereby permit tracking of people in possession of the GPS-equipped mobile phones.[48] GPS enables providers to "pin-point the position of a GPS-enabled phone anywhere on the globe."[49]

Third, radio frequency identification devices (RFID)[50] may soon be embedded in mobile phones, enabling communication between

---

Recent Development in Harvard Journal of Law & Technology, *supra* note 10, at 308–09. Signal triangulation does not yield location data as precisely as that generated by GPS systems. Duva, *supra*, at 169. One limitation of triangulation is that it does not work if the user's mobile phone is turned off. *Recent Development in Harvard Journal of Law & Technology*, *supra* note 10, at 309.

47. 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). 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. *Recent Development in Harvard Journal of Law & Technology*, *supra* note 10, at 308. 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 in conjunction with 911 emergency services. *See* Villoch III, *supra* note 18, at 448–49.

48. *See id.*

49. *Recent Development in Harvard Journal of Law & Technology*, *supra* note 10, at 308.

50. RFID systems have three components: a tag, a reader and a database. Laura Hildner, *Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level*, 41 HARV. C.R.-C.L. L. REV. 133, 134–35 (2006). First, a silicon chip and antenna combination [hereinafter RFID tag] is attached to or incorporated into consumer goods (including a mobile phone). *Id.* 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). *Id.* The RFID tag may be very small, as small as a grain of sand, and thus unnoticeable by consumers. *Id.* The tag's antenna transmits the tag's particularized information. *Id.* Second, RFID systems include a RFID reader (reader). *Id.* Readers use radio waves to scan tags to obtain their data. *Id.* Readers may be mobile or stationary and come in variable sizes and powers. *Id.* A tag used for commercial purposes generally does not have a battery, operates at ultrahigh frequencies, such that readers can access them within a few feet. *Id.* RFID systems have an advantage over EPC systems because the RFID reader can read information from RFID tags even if the RFID tag is not in their line of sight and the reader can process multiple RFID tags at the same time. *Id.* Third, RFID systems include a database. *Id.* The RFID database receives the information programmed onto RFID tags that has been read by the RFID reader. *Id.* The RFID database can link information received from the RFID tag to product information and potentially to information about the person who possesses the consumer item with the RFID tag. *Id.* For a detailed overview of consumer applications of RFID technologies, *see* U.S. Fed. Trade Comm'n, *Radio Frequency Identification: Applications and Implications for Consumers, A Workshop Report from the Staff of the Federal Trade Commission* (2005), http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf [hereinafter *FTC Workshop Report*].

advertisers and consumers with RFID-equipped phones.[51] Consumers' use of RFID-equipped mobile phones in combination with the strategic placement of RFID readers in the consumers' environment (for example, in a shopping center) will enable advertisers to track the location of consumers as they move throughout communities, collecting data about consumers' behavior in the environment and delivering advertising to consumers on their mobile phones that is targeted to a consumers' geographic location at a specific time.[52] 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 the collector and other parties, including advertisers.[53] Of course, the location data will probably

51. David Meyer, *Operators Want RFID in Phones*, ZDNET.CO.UK (2006), http://news.zdnet.co.uk/communications/0,1000000085,39284785,00.htm (reporting that the GSM Association (GSMA), representing operators that service more than 82 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. *Id.* 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 user's choice of music on the car stereo. *Id.* 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. 0020 (2005) (reporting on the emerging trend of integrating RFID in mobile handsets). *See also* Beth Bacheldor, *Nokia Uses RFID-Enabled Phones to Police Its Security Guards*, RFID J., Dec. 18, 2006, http://www.rfidjournal.com/article/articleprint/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 and enable the company to track its security guards as they patrol buildings, parking areas and common grounds); Bacheldor, *supra* note 7 (discussing the models of RFID-enabled handsets that have been issued by Nokia since 2005). Nokia's latest model that is a NFC-enabled handset containing an RFID module that can function as an RFID tag and as an RFID reader and supporting peer-to-peer communication. Bacheldor, *supra*.

52. *See generally* Katina Michael, *Trends in the Selection of Automatic Identification Technology in Electronic Commerce Applications*, Faculty of Infomatics—Papers, Univ. of Wallongong 8–9 (2003), *originally published as* Michael, K, *Trends in the Selection of Automatic Identification Technology in Electronic Commerce Applications* 135–52, *in* BUILDING SOCIETY THROUGH E-COMMERCE: E-GOVERNMENT, E-BUSINESS AND E-LEARNING, (N. Cerpa & P. Bro eds., Univ. of Talca, Chile, 2003)), *available at* http://ro.uow.edu.au/infopapers/375. Michael provides a case study about the use of RFID transponders attached to animals to track them in an environment embedded with RFID readers and discusses the convergence of RFID and other auto-identification technologies that is occurring in e-commerce applications. *Id.* Auto-identification technologies, including RFID, can also be used to track consumers' locations and deliver advertising to their mobile phones. *See infra* Part III for discussion of the BART RFID Trial that is based on consumers use of RFID-equipped mobile phones in combination with the strategic placement of RFID readers in the consumers' environment that enable advertisers to track the location of consumers as they move throughout the environment and to deliver advertising to consumers on their mobile phones based on the consumers' geographic location at a specific time.

53. U.S. GOV'T ACCOUNTABILITY OFFICE, RADIO FREQUENCY IDENTIFICATION TECHNOLOGY IN THE FEDERAL GOVERNMENT 9, GAO-05-551 (May 2005), *available at* http://

only be useful for delivering LBS and other advertising for a limited time period because consumers also are mobile and will not likely remain at a specific location very long.

Given this Article's focus on the privacy implications of providing RFID-enabled phones to consumers, it is important to discuss how these phones will enhance the ability of advertisers to deliver mobile advertising to consumers. The International Telecommunications Union (ITU) is a specialized agency of the United Nations for information and communications technologies.[54] It has issued a report explaining opportunities presented by RFID for mobile telecommunications services. This report explains how RFID-enabled mobile phones may soon provide consumers with new services.[55] The report specifies that RFID-based mobile communications services can be used to provide information on objects equipped with an RFID tag over a telecommunications network. Once a mobile phone is equipped with an RFID reader it can retrieve information on tagged items which is stored in a database and is accessed via the mobile network.[56] The report explains how advertising can be delivered to mobile RFID-enabled mobile phones:

> Information retrieval via RFID enabled mobile phones could be used for advertisements. Posters or paper-copies of advertisements could carry a small RFID-tag. Anybody interested in more information on the advertised product or event would just have to hold his mobile phone close to the tag. The information would then again be retrieved from a database. The delivered information could also be multimedia-content: For example, the RFID equipped cell phone could provide a free preview of a movie when the user reads an RFID tag that is attached to the movie poster.[57]

Furthermore, the presence indication capability of RFID can be used to produce automated messages to mobile phones whenever the mobile phone comes near an RFID reader, so presumably these messages could be advertising messages.[58] For this purpose:

> [T]he RFID equipped mobile phone does not act as a reader but carries an RFID tag. RFID equipped cell-phones might thus

---

www.gao.gov/new.items/d05551.pdf (providing an exhibit showing the components of an RFID system that includes storage of data in databases that are connected to the Internet).

54. *See* International Telecommunications Union, http://www.itu.int/net/home/index.aspx (last visited Jan. 4, 2009).

55. *See generally* Seidler, *supra* note 2.

56. *Id.* §§ 3, 3.1.1.

57. *Id.* § 3.1.1 (citation omitted).

58. *See id.* § 3.1.6.

> have to be equipped with both a reader *and* one or multiple RFID tags . . . . [T]he RFID tag on the phone would then enable readers in the environment to identify the phone—and respectively the person carrying it.[59]

The report also explains the relationship between Near Field Communications (NFC) technology and RFID, indicating NFC is not equal to RFID services in mobile networks, but is instead a subset of it.[60] The NFC communications protocol is a concept already used for RFID-enabled mobile phones.[61] The NFC communications protocol has not yet been widely adopted by handset manufacturers who are engaged in mass production of cell phones, and no mobile operators have yet bought the phones to promote NFC services to their customers.[62]

The Report's discussion of the use of RFID to provide new services for consumers and advertising opportunities assumes the information retrieval and presence indication capabilities of RFID will be used in conjunction with a telecommunications network. But from a regulatory compliance standpoint, what if m-advertisers used RFID-embedded environments like shopping centers and bus stations to communicate their m-ads directly to consumers who have RFID-enabled mobile phones without using the telecommunications network? And what if RFID-enabled phones were the industry-standard for mobile phones such that many or most mobile phones sold to consumers were already equipped

---

59. *Id.*

60. *Id.* § 3; *see also* INNOVISION RESEARCH & TECH. PLC, NEAR FIELD COMMC'N IN THE REAL WORLD § 2.3 (Dec. 2007) (on file with author) (describing how NFC works).

61. Seidler, *supra* note 2, § 3.2. The NFC protocol is an ISO/IEC 14443 compatible short-range communication protocol operating over distances of a few centimeters, which uses the 13.56 MHz high frequency range. *Id.* "The reader provides power to the chip in the passive RFID tag by inductive coupling." *Id.* A report by ABI Research "gives NFC-enabled mobile phones a market share of fifty percent by the year 2009." *Id.*

62. NFC is still an emerging technology that could have a bright future building on the infrastructure already used in Europe to enable people to use their mobile phones to make contactless payments for transportation, groceries, movie admissions and other services. *See* Jonathan Collins, *Could NFC Fail to Take Off?*, RFID J., Apr. 7, 2008, http://www.rfidjournal.com/article/articleview/4005/1/128 (arguing that the lack of current adoption of NFC protocols in mobile phone handsets are a "reflection of the business issues and partnerships required for NFC payment applications, not a judgment on the potential of the technology."). The emergence of mobile phones equipped with RFID modules compliant with NFC specification is expected to boost the popularity of contactless payments. Mary Catherine O'Connor, *RFID Payment Fobs Fail to Woo Consumers*, RFID J., Apr. 4, 2008, http://www.rfidjournal.com/article/articleview/4002/1/1/. Nokia produces RFID-enabled mobile phone handsets and is scheduled to begin shipping its fourth generation RFID-enabled handsets using NFC protocol in Fall 2008. Bacheldor, *supra* note 7. A partnership between Visa and Nokia has been announced to enable Visa to offer RFID-enabled services such as contactless payments utilizing Nokia's newest model of RFID-enabled mobile phones, although a spokesperson for Visa said the company has immediate plans to develop payment-related services to leverage the peer-to-peer communications features in the new phones. *Id.*

with RFID tags and readers to facilitate the delivery of LBS and m-advertising messages to consumers?

Existing government regulation of telecommunication carriers in both the United States and Europe already address, to some extent, the privacy and data protection concerns associated with location tracking technologies that utilize GPS or cell phone triangulation.[63] However, technologies like RFID-enabled mobile phones make it possible for mobile advertisers to deliver m-advertising without using the services of highly regulated public carriers, thus undermining the current regulatory framework that focuses on public carriers. When consumers have RFID-enabled mobile phones and shopping centers and bus stations are embedded with RFID technologies, mobile advertisers will be able to track consumers through their phones and deliver m-advertising directly to the phones through contactless wireless communications that do not require use telecommunications networks. Accordingly, this paper analyzes the adequacy of government regulation in the European Union and United States to protect consumer privacy and data protection in emerging m-advertising contexts that involve consumer tracking facilitated by RFID technologies.[64]

III. Mobile Phones Combined with RFID Technologies Create Value But Also Raise Privacy Concerns

For both businesses and consumers, there are benefits to be gained when consumers have mobile phones that are equipped with RFID technologies and the business environment is equipped with RFID readers and tags. But there are also privacy and data protection concerns. When RFID systems are used to deliver LBS and mobile advertising, there is the potential for consumers to be unaware of privacy-intrusive nature of these systems. One of the distinguishing characteristics of RFID systems and other AmI systems is that they may lack transparency from a privacy perspective, meaning that RFID systems may operate automatically and

63. *See* discussion *infra* Part VII (reviewing the existing E.U. and U.S. regulatory frameworks for RFID applications).

64. Work by previous scholars on consumer privacy issues related to RFID is the starting point for this study. *See, e.g.*, Stein, *supra* note 2, ¶¶ 35–40 (2007) (proposing to amend existing U.S. laws, which the author concludes are insufficient to address consumer privacy concerns related to the broad use of RFID technology in supply-chain and other contexts); Eden, *supra* note 51, at 29 (arguing for amendments to the Privacy Act of 1974 to require corporations to preserve individual anonymity with respect to consumer privacy preferences). This study differs from previous work on this topic because it utilizes a comparative law approach with a focus on E.U. and U.S. law and because it focuses on RFID use in mobile phones, as opposed to broader focus on use of RFID in the supply chain or the broad use of RFID in consumer products.

invisibly in the background, resulting in a form of secret surveillance.[65] Furthermore, to the extent that RFID systems gather, store and use personal data, they may not provide appropriate notice and consent features from the perspective of fair information practices. Recent consumer trials testing systems using RFID-equipped mobile phones for m-commerce transactions help provide a context for discussion of the potential risks from the perspective of privacy and data protection.[66]

One such consumer trial in the United States features the use of RFID-equipped mobile phones by San Francisco commuters who use Bay Area Rapid Transit ("BART" and "BART RFID Trial").[67] More than 200 San Francisco-area commuters, who were already subscribers of Sprint mobile phone service, have agreed to use Sprint's RFID-equipped cell phones.[68] In the trial, these commuters are able to use their phones to pay fares on the local subway system, to download directions to the nearest Jack in the Box fast food restaurant and to pay for their pur-

65. Mireille Hildebrandt, *Profiling into the Future: An Assessment of Profiling Technologies in the Context of Ambient Intelligence*, 1 FIDIS J. OF IDENTITY IN THE INFO. SOC'Y 7 (2007), http://journal.fidis.net.

66. *See* Claire Swedberg, *Cell Phone Service Providers Start Global NFC Initiative*, RFID J., Feb. 6, 2008, http://www.rfidjournal.com/article/articleview/3893/1/1/ (describing the launching of a NFC mobile phone pilot titled "Pay-Buy-Mobile" in France, Taiwan and Turkey, with plans to expand the trial to eight more countries this year). In the trials, local banks and credit card companies partner with mobile service companies and phone manufacturers to provide sample groups of consumers with NFC-enabled mobile phones they can use to purchase goods and services from participating vendors. *Id.*

67. Mary Catherine O'Connor, *SF's Transit System Offers Commuters Fast Access to Subways and Sandwiches*, RFID J., Jan. 31, 2008. The trial also involves mobile phones equipped with Near Field Communications (NFC) technology, which is a wireless technology that uses a high-frequency RFID protocol to exchange data through RFID modules embedded in electronic devices such as cell phones. *Id.* The businesses participating in this trial include: BART (configured the database); First Data (providing payment processing services for the trial); ViVOTech (providing online registration to create debit or credit accounts for customers for the trial and provides software to power the RFID application inside the cell phones); and Samsung (manufacturer of RFID-equipped handsets). *Id.* Also, NXP Semiconductors (developed the chips for the Sprint NFC enabled mobile phones to facilitate secure, contactless communication between the mobile devices and BART's fare gate readers). *See* Press Release, BART Trial First To Use Mobile Phones to Pay for Fares & Food, ViVOTech (Jan. 29, 2008), http://www.vivotech.com/newsroom/press_releases/BART_trail_release.asp [hereinafter *ViVOTech Press Release*] (announcing that "participants can hold their specifically-equipped Sprint mobile phone up to certain Jack in the Box® and Sprint 'smart advertisements' on BART station walls and download either directions to the nearest Jack in the Box restaurant or content from Sprint").

68. Sprint, a leading mobile telecommunication carrier in the United States, is involved in the trial through its existing relationships with consumers—only subscribers of Sprint's mobile telecommunication services were invited to participate in the trial. O'Connor, *supra* note 67. In the trial, Sprint also delivers content to participants. *See ViVOTech Press Release*, *supra* note 67.

chases at Jack in the Box locations.[69] In return, trial participants receive mobile advertising.[70] To participate, a commuter must have a mobile phone that has been embedded with a RFID module.[71] The system also requires RFID readers and RFID tags to be incorporated into the physical environment where consumers will use the phones. In this case, the environment already contained some of the RFID technology needed for the trial because the subway turnstiles in the subway stations had already been equipped with RFID readers that were installed in 2006 to facilitate BART's EZ Rider program. The EZ Rider Program allows frequent BART commuters to pay for their fares using RFID-enabled plastic cards: a commuter pays his fare through a debit account that is created and linked to the ID number encoded in the inlay on the commuter's card.[72]

In the 2008 trial, the RFID-enabled plastic card was replaced by a cell phone embedded with an RFID module. Smart posters inside the BART station allow the commuters to get directions to the nearest Jack in the Box Restaurant and to access content provided by Sprint, including advertisements. For example, the smart posters featuring Jack in the Box restaurants have RFID tags embedded in them; commuters use their phones equipped with an RFID reader to collect a URL from the tag on the poster and then the phone's Web browser calls up the Web page for the URL to display the nearest restaurant location.[73] Once at a Jack in the Box restaurant, RFID readers installed in Jack in the Box Restaurants allow commuters to pay for their orders by holding their phones close to RFID readers.[74] RFID technology installed in Jack in the Box restaurants is used to capture the commuters' purchases.[75] Commuters get a receipt from Jack in the Box when their orders are complete.[76] A database holds participants' account IDs and links their user accounts to payment

69. This test of NFC technologies in both a mass transit and a retail environment is expected to run for several months in 2008. *Id.*

70. *Id.*

71. O'Connor, *supra* note 67 (reporting that the specific RFID technology used in the trial is a NFC module). Samsung handsets are being used in the trial; however Samsung does not currently sell RFID-enabled handsets to the public in the United States. *Id.* Nokia offers an RFID-enabled model in the United States and Europe and RFID-enabled phones are widely used in Asia. *Id. See also RFID in Japan: Japan's Experience with RFID Phones and Contactless Cash*, DIGITAL WORLD TOKYO, Apr. 30, 2008, *available at* http://www.digitalworldtokyo.com/index.php/digital_tokyo/articles/rfid_japans_experience_with_rfid_phones_and_e_cash/.

72. O'Connor, *supra* note 67.

73. *Id.*

74. *Id.*

75. *Id.*

76. *Id.*

processing services.[77] Commuters have the option to set up a personal identification number which they would need to key-in before accessing the system, but unless they do so, they will be able to just press one button on their phones and then hold their phones up to the payment terminal.[78] If a commuter loses his phone, the commuter may contact Sprint to have the phone deactivated.[79]

In the trial, consumers benefited in several ways: they saved time by avoiding the need to wait in line to purchase tickets to get on the subway, they did not need cash or correct change to purchase their subway tickets, they were able to get directions to Jack in the Box to buy food, thus saving time finding a restaurant, and they were able to buy food quickly at Jack in the Box restaurants without having to carry cash. To the extent that consumers welcome relevant advertising, they also benefited by having access to advertising or other content available through Sprint's smart posters in the subway, perhaps being able to view movie previews or access special offers. Essentially, their phones became a source of LBS services to pay for subway tickets and food and to obtain directions, as well as providing a source of m-advertising content. Among the advantages to participating businesses were enhanced efficiency of operations, including cost savings, boosting the number of riders on the subway and visitors to participating restaurants, having better data about their customers and having a ready mechanism to deliver m-advertising.

Personal data used in the BART RFID Trial included location data to enable tracking of commuters. To illustrate, location data about a commuter will be generated whenever a commuter's phone is held close enough to an RFID reader to be read (at the subway turnstile or in the Jack in the Box restaurant when payment is made) or when the commuter's RFID reader is held up to a smart poster to get directions or access other special ads and offers from Sprint. Information about commuters will also be generated by the system, such as what they buy or when they travel, and linked to a particular commuter by his unique identification number. In the current trial, commuters must take the initiative to obtain the advertising content by holding their RFID-equipped mobile phones near smart posters in the BART stations.[80] However it is not difficult to imagine how advertising could instead be marketed to consumers. For example, when a commuter pays for his subway ticket or food purchases, RFID readers used to process the purchases can send advertisements to the consumer along with confirmation of his purchase,

77. *Id.*
78. *Id.*
79. *Id.*
80. *See id.*

perhaps via his telecommunications service. Location and other personal information gathered in the BART RFID Trial could be used to target other advertising to individual consumers based on market or consumer behavioral analysis and on a time and location specific basis.

Ongoing consumer trials, such as the BART RFID Trial, demonstrate that now is the time to address the consumer privacy and data protection concerns associated with bringing new RFID-equipped mobile phones and location-based services to the market. There is still time to design the technology and supporting regulatory systems to protect consumer privacy interests.

IV. The Challenges of Finding Common Solutions to Protect Consumer Privacy and Facilitate M-Commerce

The significant privacy and data protection concerns associated with consumers' use of RFID-enabled mobile phones are part of broader privacy concerns relating to our current information age that feature ambient intelligence and autonomic computing.[81] In "The Internet of Things," the future made possible by emerging technologies such as RFID systems, sensors, smart technologies and nanotechnologies is envisioned to be one with autonomic computing environments that produce and use ambient intelligence.[82] In an ambient intelligence (AmI) environment, humans are surrounded by pervasive, ubiquitous and interconnected computers that anticipate their preferences in order to adapt their environment to their inferred wishes.[83] Autonomic computing

81. With autonomic computing systems, "[s]ystems manage themselves according to an administrator's goals. New components integrate as effortlessly as a new cell establishes itself in the human body. These ideas are not science fiction, but elements of the grand challenge to create self-managing computing systems." Jeffrey O. Kephart & David M. Chess, *The Vision of Autonomic Computing*, Computer Mag., Jan. 2003, at 41, http://www.research.ibm.com/autonomic/manifesto/ (attributing the term "autonomic computing" to Paul Horn, who introduced it in his March 2001 keynote address to the National Academy of Engineers at Harvard University); *see also* Paul Horn, Autonomic Computing: IBM's Perspective on the State of Information Technology 6 (2001), http://www.research.ibm.com/autonomic/manifesto/.

82. *The Internet of Things*, *supra* note 1, at 9–40.

83. Hildebrandt, *supra* note 65, at 7 (describing the key elements of Ambient Intelligence and citing The New Everyday, Views on Ambient Intelligence (E. Aarts & S. Marzano eds., Rotterdam 2003) as a source of previous definitions of this term). According to Hildebrandt, the key elements of an ambient intelligence (AmI) environment are that computerized devices are:

- •embedded (many networked devices integrated into the environment)
- •context-aware (these devices recognize you and your situational context)
- •personalized (they can be tailored towards your needs)

technologies are a precondition for creating ambient intelligence, and RFID is one of the autonomic computing technologies upon which the vision and creation of ambient intelligence rests.[84]

As described in Exhibit A, there are at least six distinct consumer privacy concerns that arise when RFID-enabled mobile phones are used to deliver location-based services and m-advertising. These six consumer privacy issues are: data protection, tracking, spamming, skimming and eavesdropping, profiling using personal data, and profiling using anonymous data.[85]

EXHIBIT A
KEY PRIVACY ISSUES FOR CONSUMERS:
WHEN MOBILE PHONES ARE RFID-EQUIPPED AND USED TO DELIVER
LOCATION-BASED SERVICES AND MOBILE ADVERTISING

Privacy Risk	Explanation & Examples
1. Data Protection The potential for advertisers and other third parties to collect consumers' personally identifying information from the RFID tags in their phones. However, if a read-only function is assigned to the RFID-reader in the phone and the reader does not communicate a unique identification of the phone in the process of reading a tag in the user's environment, use of the phone as a reader does not raise data protection issues because this process should not reveal any personal information.	-Product identification information similar to the type of information on a bar code; for example, a unique identifying number for each mobile phone and the phone's model number, which are not personally-identifying data unless it is linked to an individual person. -Other types of personal information that could be stored on RFID tags in mobile phones: consumer's name, address, mobile phone number, date of purchase, method of payment (although it is not necessary to store this type of information on an RFID tag as it could be stored in a separate database that is linked to the phone via a unique identification number). -Other types of personal information stored on the consumer's mobile phone apart from the storage capacity of the RFID tag that could be accessed by hacking the phone's memory include: the user's list of contacts, passwords for accounts, messages, etc.

•adaptive (they may change in response to you)

•anticipatory (they can anticipate your desires without conscious mediation).

Id. at 7. "Other key elements . . . are: hidden complexity; the absence of keyboards or monitors, the fact that the environment itself becomes the interface, real time monitoring and proactive computing." *Id.*

84. *Id.* For an explanation of the term "autonomic computing," see Kephart & Chess, *supra* note 81, at 41.

85. *See* Exhibit A, *infra*. Two types of consumer profiling are discussed in this exhibit that are distinguished by whether the profiling uses personal data or instead uses anonymous data. *See id.* at items 5 and 6.

Privacy Risk	Explanation & Examples
2. Tracking The potential to reveal the geographic location of the consumer by virtue of location tracking capabilities related to having an RFID-equipped phone with an RFID tag that transmits a unique identifying number, which may be enhanced by having a phone that has also been equipped with other location tracking technologies (e.g., GPS).	-RFID readers in the consumer's environment will detect the presence of the RFID tags in the user's phone—since the phone must be within the read range of the reader for this to occur, the reader will capture information about the user's geographic location at a specified time. -Also, when the consumer uses his mobile phone to read a smart poster and then moves to another location to purchase a product using his RFID-equipped phone, his geographic location may be captured by the RFID-system that he is interacting with and can be stored in a database. -GPS data about the location of a mobile phone user could be combined with the RFID-captured data about the consumer's location for more complete tracking data about the consumer's location at specific times.
3. Spamming The increased risk of receiving unsolicited m-advertising (e.g., voice telemarketing calls, SMS or text-message ads, multi-media ads, pop-up or banner ads generated by their phones). Also, the increased risk of having adware or spyware software downloaded on their phones that could be used as a mechanism to deliver spam.	-When the consumer uses his mobile phone to make a contactless payment transaction, the mobile phone's RFID-reader may access mobile spam or a subsequent confirmation of a payment transaction sent to the mobile phone may be accompanied by mobile spam (e.g., text, multi-media, banner, pop-up spam to be displayed on the phone). -Advertisers who have knowledge of the consumer's mobile phone number may generate text messages and other forms of advertising spam to consumers that are location and time specific facilitated by RFID-readers in the consumer's environment that detect the consumer's location and are able to identify the phone's user. -The phone's RFID reader is a new potential portal for adware and spyware software downloads to the phone that may thereafter be used to generate m-ads to the phone. If the download is without adequate notice and consent, this creates a portal for spam.

Privacy Risk	Explanation & Examples
4. Skimming & Eavesdropping The risk that consumers' personally identifying data stored on their phones will be accessed by others without authorization or that transmissions of personal data will be intercepted while it is in transit by unintended and unauthorized parties (e.g., rival advertisers, criminals engaged in identity theft or fraud).	-Depending on the types of data recorded on RFID tags in mobile phones and/or the security risks associated with having RFID-readers in the phones that can be hacked in order for an outsider to access other personal data that is stored on the phones, consumers' personal data may be accessed while it is in electronic storage by persons without authorization (skimming). -Alternatively, personally identifying information could be intercepted without authorization while it is in the process of being communicated between an RFID tag and an RFID-reader (eavesdropping). -Due to the contactless nature of RFID and the fact that RFID-systems operate autonomously in the background without the user's intervention, the mobile phone user may not be aware of the leak of his personal data. -If the data on the RFID-tag is encrypted, this may prevent breach of personal data stored on the tag, but skimming & eavesdropping may still be used to track the phone if the tracker can uniquely identify one phone from another.
5. Profiling Using Personal Data The risk that consumers' personal data will end up in commercial data banks and be added to consumer dossiers by virtue of the ability of RFID systems to collect data automatically and to then communicate that data easily over the Internet. Effectively, a consumer may lose control of the collection and sharing of his personal data, raising the risk of identity theft and fraud.	-Because RFID-systems can store personal data in databases that can be connected to the Internet, any data in digital form can be processed using data mining techniques to create consumer dossiers and can be shared with others through access to the database or transferring the data to other databases. -Examples of the types of data that could be stored, analyzed, shared include: location data and other personally-identifying data about consumers with mobile phones including data collected by virtue of the RFID-enabled phone as well as other data. Such data may or may not be made anonymous at the time of collection or thereafter.

Privacy Risk	Explanation & Examples
6. Profiling Using Anonymous Data The risk that data about consumers will be gathered and used to create group profiles that are applied to groups of consumers in order to generate targeted marketing to desirable groups of consumers according to the marketer's objectives. The privacy concern to consumers is the lack of transparency of the process if consumers are not given access to information about the knowledge profiles that are applied to them and that determine whether or not they are being included or excluded from receiving favorable marketing opportunities, etc.	-Consumer is included in a favorable group profile/classification; e.g., receives mobile advertising that will grant him a favorable purchasing opportunity compared to other consumers who are not in the favorable classification, such as a discounted price on an item he is interested in purchasing. -Consumer is excluded from a favorable group profile/classification; e.g., does not receive a favorable purchasing opportunity compared to other consumers who are in the favorable profile, so, for example, he must pay a higher price to purchase an item that he is interested in compared to other consumers that are in the favorable classification.

The starting point for resolving each of these important privacy challenges is recognizing that they arise in the context of ambient intelligent systems. An essential component of ambient intelligence systems is information about users, so, from a consumer privacy perspective, some argue it is likely that losing control over one's personal information is an unavoidable cost of entering into an AmI world.[86] Such a world, characterized by pervasive and invisible information systems that constantly and automatically record events that occur there, makes it highly unlikely that individuals who enter will retain control over how their personal information is processed. Understanding the ubiquity and invisibility of computers operating in AmI environments is critical to addressing the risk of eavesdropping and skimming for consumers using RFID-enabled phones because it means that consumers are not well-situated to prevent or detect data and communication leaks.[87] Additionally, spamming, the vexing problem of unsolicited electronic communications, is expected to be a problem not only for those using Internet-connected computers, but also for mobile phone users. This is a key privacy issue as mobile phones are now an essential and very personal communications device that consumers are likely to have with them nearly all of the time. Mobile phones are a convenient portal to the AmI era and the benefits of new location-based services. Yet that convenience will be lessened if it comes with interruptions of personal time

86. *See* Rouvroy, *supra* note 14, at 8–9.
87. *See EPIC Testimony on AK RFID Bill*, *infra* note 108, at 3.

and space in the form of increased spam made possible by RFID-enabled mobile phones and RFID-embedded environments.

Finally, the privacy risks related to consumer profiling take on more importance in AmI environments. As Rouvroy argues, the "reasons that privacy issues are so vividly debated on the threshold of an 'AmI era' go well beyond . . . important concerns for control over personal information (data protection)" and include discussions about the impact of AmI on individual privacy.[88] One significant privacy impact identified by Rouvroy relates to the impact on individual autonomy that occurs from the classifications of people that occur in an AmI environment.[89] For example, consider one AmI scenario: an RFID system installed in a shopping center for marketing purposes that is designed to focus on consumers carrying RFID-enabled mobile phones. A primary goal of such a system is to classify consumers for a variety of marketing purposes, such as their willingness to buy certain products.[90] Although such a system may be designed to aid the customer by automatically displaying information optimized to the consumer's needs or preferences, as interpreted by the system, the benefit to the consumer depends on how the system classifies that consumer, and whether the system changes the classifications as a result of consumer response. This process has been called "making up people."[91]

The privacy concern for the customers in this AmI scenario involving RFID and mobile marketing is not merely that tiny details of their lives, such as shopping habits or movements within a shopping area, are being observed, but rather that meaning may be accorded to these small details captured by the system. So, the probable impacts of AmI are less about discovering what is preexisting about the consumer and more about creating new interactions and behaviors involving the customer and the marketer. These new interactions are produced through the "interplay of statistics and correlations" that produce or reinforce "*norms*, the criteria of normality and desirability against which individual life-

88. *See* Rouvroy, *supra* note 14, at 9.

89. *Id.* at 14.

90. Viewed from a privacy perspective, consumers in this mobile marketing scenario are the objects of "scientific or bureaucratic inquiry for a variety of purposes going from controlling to helping them," and the result is classification of people that affects the people classified, and, in turn, the classifications are changed by the system to reflect the changes in the people produced by the classifications. *Id.* at 16.

91. Ian Hacking, "*Making Up People"*, LONDON REV. OF BOOKS 23–26 (Aug. 17, 2006) (reprinted from IAN HACKING, HISTORICAL ONTOLOGY 99–114 (2002)) (discussing how people are moving targets in scientific investigations that classify people; such investigations interact with them and change them, and since they are changed, the people are not quite the same kind of people they were before, and so the target of the investigation has moved, a process Hacking calls the "looping effect").

styles, preferences, choices and behaviors will be evaluated."[92] AmI classification systems are designed to reward consumers who are compliant with these norms, but sanction deviant consumers, e.g., by discriminating among consumers in terms of providing increased or reduced access to specific places, goods, services, activities or other opportunities.[93] Analysis of the role of law in this new context requires considering whether individuals should have access to the classifications that are applied to them in order to exercise individual rights of self-determination and to enable them to effectively participate in the democratic processes that ultimately legitimize or constrain uses of such classifications.[94]

The advent of RFID-enabled mobile phones gives us a context for privacy discussions that is broader than whether law should protect personal data. This presents an opportunity to work towards global solutions that may not be possible in the context of data protection alone. As such, the discussion is really about trade-offs between protecting the personal liberty of consumers and the freedom of businesses to participate in commerce and to market their products and services. Protection of personal liberty is an essential principle found in the legal systems of both the European Union and the United States.[95] Arguably, even if the European view that protection of personal data is necessary as a fundamental right is never adopted into U.S. law, it may be possible to reach workable privacy solutions because both legal systems place a high value on protecting personal liberty.

---

92. Rouvroy, *supra* note 14, at 16–17.

93. *Id.*

94. Rouvroy says:

> The central importance of privacy and data protection in the context of AmI is thus not merely due to the fact that AmI systems record what happens in "real life." What is crucial here is that those systems "construct" . . . the meaning of those events and, on the that basis, frame the user's environment in ways that in turn impact . . . self-perception, choices, preferences and behaviors, interfering . . . with the effective exercise by individuals of their capacity for self-determination.

Id. at 17 (arguing that "to the extent that those classifications condition access or denial of access to valuable opportunities in life, they should result from a democratic deliberative process." *Id.* at 18). Rouvroy says that AmI systems are problematic from an ethical and legal perspective because such systems fail to respect individual autonomy. AmI systems produce "knowledge . . . about users on the basis of correlated data [that] transforms the subjects about whom that knowledge is constructed," turning the user's position as a "subject" into a position of being an "object." *Id.* at 18.

95. *See generally* Nancy J. King, *Fundamental Human Rights Principle Inspires U.S. Data Privacy Law, But Protections Are Less Than Fundamental*, *in* CHALLENGES OF PRIVACY AND DATA PROTECTION LAW, PERSPECTIVES OF EUROPEAN AND NORTH AMERICAN LAW, 71–98 (Centre de Recherches Informatique et Droit (CRID), Maria Veronica Perez Asinari & Pablo Pallazzi, eds., Bruylant 2008).

A. *Data Protection*

When businesses use consumers' personal data, questions of information or data privacy arise.[96] Generally speaking, personal data are information that are specific to individuals, such as the person's name, address, phone number, sex, age, marital status, and income.[97] Protecting the privacy of personal data and associated fair information practices are recognized as being important to society and to the development of global commerce.[98]

Principles of fair information practices for the protection of personal data 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 that have implemented the Data Protection Directive in the European Union or the Customer Proprietary Network Information ("CPNI") rules under the federal Communications Act and related binding administrative rules in the United States);[99] (2) policy statements of

---

96. *See, e.g.*, Joel R. Reidenberg, *Symposium: Cyberspace and Privacy: A New Legal Paradigm? Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1325–26 (2000) (using the terms "data protection," "data privacy," and "information privacy" interchangeably to describe the same types of government regulation). Data privacy, also called information privacy in the United States, has been described as:

> One of the branches of the legal right to privacy . . . concern[ing] itself with the extent to which persons are able to limit access to information about themselves. The right is expressed as a person's right to "control," "limit access to," or "determine for themselves when, how, and to what extent information about them is to be communicated to others."

See Richard C. Turkington, Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy, 10 N. ILL. U. L. REV. 479, 487 (1990).

97. *See, e.g.*, Organisation for Economic Co-operation and Development [OECD], *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2001), http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html [hereinafter *OECD Privacy Guidelines*]. According to the OECD Privacy Guidelines, "personal data means any information relating to an identified or identifiable individual". *Id.* § 1(b). *See also* Council Directive 94/46, art. 2(a), 1995 O.J. (L 281) 31 [hereinafter *Data Protection Directive*] (defining "personal data" to include, data about natural persons "who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.").

98. *See, e.g.*, Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 730–31 (2001) (commenting that there is a "consensus among democratic states that information privacy is a critical element of civil society."); Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1325 (2000) (commenting that "democracies converge on a basic set of principles for 'data protection' or 'data privacy'. These norms of fair information practice constitute what can be termed First Principles, and their acceptance separates democratic societies from totalitarian regimes").

99. *See generally supra* note 97.

government agencies that are advisory but not legally binding (in the United States, the Federal Trade Commission's ("FTC") fair information principles of notice, consent, access, security, and enforcement);[100] 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).[101] In the United States and the European Union, some consensus appears to exist on the basic components of fair information practices. For example, 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 his personal data by any entity collecting the data. But the advent of RFID-enabled phones and RFID-embedded environments creates significant challenges in giving notice and obtaining consent. These challenges include the invisibility and autonomous operation of RFID technologies from the consumer's perspective; this is characterized by contactless communications between devices that can operate automatically in the background without user involvement. Another challenge is the consumer's difficulty in using a small mobile device to receive and review privacy notices and to indicate consent. And, if the consumer receives the notice but does not wish to consent, how may the consumer protect his privacy in an RFID-enabled environment without leaving his mobile phone elsewhere? Will the RFID-equipped device have an off-button? Can the consumer choose to have the RFID module permanently or temporarily disabled?

To the extent that RFID systems use or generate personally-identifying information about consumers, they raise questions of personal data protection, but not all uses of RFID involve personal data. In some situations there is no ambiguity about whether an RFID system uses personal data—such is the case with many RFID systems that use personal data like an identification number to control access by persons

---

100. FTC, Fair Information Practice Principles [FTC's FIP], http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited Jan. 16, 2009). The second principle, Choice/Consent, includes obtaining consumer consent about how information collected from them may be used. *Id. See generally* King, *supra* note 95, at 71–98.

101. *OECD Privacy Guidelines*, *supra* note 97. *See also* Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, 44 AM. BUS. L.J. 55, 61 n.26 (2007) (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).

to a facility or service.[102] When an RFID system makes it possible to link non-personal data to an identified individual, the system uses personal data.[103] For example, RFID systems used in supply-chain systems may store a unique number on an RFID chip attached to a box of product in order to identify it and track it. This system does not use personal data because none of the data used is about an individual person. But if the unique number stored on the RFID chip is collected or processed to enable association of the number with an individual person, then it can become personal data.[104] Furthermore, access to information on a RFID tag may reveal information about the person carrying an object with an RFID tag even if no personal information is stored on the tag, and sometimes this information can be quite sensitive. For example, it could be inferred that a person carrying a specific medication, identified through an RFID tag on the container in which the medicine is stored, has an associated medical condition.[105] In the context of a mobile phone, assume an RFID tag built into the phone contains typical electronic product code information, such as the identity of the manufacturer of the phone, the type of product (e.g., model number), and a unique serial number for the phone.[106] If the RFID tag is read by a third person like a marketer, it will reveal that a person is carrying a Samsung mobile phone of a certain model and with a certain serial number, but it does not contain personally-identifying information. On the other hand, when the marketer accesses a database that links the phone's serial number to its purchaser (e.g., information such as the credit card details of the phone's purchaser or the name of the purchaser in a warranty registration database), then the RFID data has become personal data.[107]

B. *Eavesdropping and Skimming*

The wireless nature of RFID technology presents a security risk for consumers because they may be unaware that their personal information

102. *OECD Report on RFID*, *supra* note 16, at 38–39, 42.

103. *Id.*

104. *Id.*

105. *Id.* at 38.

106. *Id.* Please note that the mobile phone example is the author's own hypothetical based on the OECD's discussion of the standard types of data anticipated to be included on RFID-tags on consumer devices.

107. The OECD Report discusses a grey area that relates to the possibility that the collection of a unique set of data, included in one or several different RFID tags, which could be related to a specific individual, makes the information personal data within the scope of E.U. data protection laws. *Id.* at 42. Industry representatives have challenged this interpretation and take the position that "data protection frameworks should apply only in cases where data processed through the use of RFID technology either contains personally identifiable information such as name, account or registration number or is combined with other personal data (e.g., personal data stored in a database or smart card)." *Id.*

has been stolen through skimming or eavesdropping.[108] Skimming describes a situation in which someone with an unauthorized RFID-reader uses it to obtain information from an RFID chip in a mobile phone without the mobile phone user's knowledge or consent.[109] Eavesdropping occurs when an "unauthorized individual intercepts data as it is read by an authorized RFID-reader or transponder."[110]

For a mobile phone user with an RFID-enabled phone, the privacy risks of eavesdropping and skimming occur because her phone has been equipped with an RFID tag that contains a memory chip that can store personal and other data and which can be read to reveal their contents. RFID readers in the consumer's environment are able to initiate contact with RFID tags in mobile phones as long as the tag is within the reading distance of the RFID system.[111] Generally speaking, the distance necessary to read RFID tags was initially thought to be only a few inches, but tests have shown that RFID tags can be read from thirty to seventy feet away in some instances.[112] "In the absence of effective security techniques, RFID tags are remotely and secretly readable."[113] Although the "creation of a small, easily portable RFID reader may be complex and expensive now, it will be easier as time passes," thus increasing the risk of skimming and eavesdropping.[114]

C. *Spamming*

A third 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

---

108. *See S.B. 293: Electronic Communications Devices: Hearing on S.B. 293 Before the S. Judiciary Comm.*, 25th Legis., 2008 Sess. 3 (Alaska 2008), *available at* http://epic.org/privacy/rfid/ngo_test_031708.pdf [hereinafter *EPIC Testimony on AK RFID Bill*] (prepared testimony and statement of Melissa Ngo, Senior Counsel and Dir., EPIC Identification & Surveillance Project).

109. *Id.* (defining the term "skimming" in the context of skimming RFID-chipped items such as identity or bank cards).

110. *Id.*

111. *Id.* The RFID-reader in the consumer's phone also can initiate contact with RFID tags in the consumer's environment, such as tags embedded in smart posters or product packaging, but for simplicity's sake in analyzing the privacy risks to the consumer, this detail is not discussed here.

112. *Id.* (referencing tests by the Department of Homeland Security in 2005). *See also* Ari Juels, *The Vision of Secure RFID*, 95 PROC. OF THE IEEE 1507, 1507 (2007) (commenting that "certain types of inexpensive RFID tags (with no embedded power source) are subject to reading at a distance of tens of feet.").

113. *EPIC Testimony on AK RFID Bill*, *supra* note 108, at 3.

114. *Id.*

consumers are likely to have their phones turned on and with them nearly all the time.[115] The precise question addressed here is "Is having an RFID-enabled phone for the purpose of using it to receive location-based services likely to expose consumers to more spam?"[116] There are two basic reasons that consumers have a higher risk of receiving increased spam on their mobile phones by virtue of having an RFID-enabled mobile phone. First, when the consumer uses his phone to receive location-based services, advertisers have the opportunity to send consumers advertising along with the service or information the consumer is seeking. The m-ads could accompany directions or a map that the consumer requests, and to the extent the consumer gives consent to receive the service, it may be argued he is also impliedly consenting to receipt of the advertising and, therefore, it is not spam.[117] But while the consumer has his phone turned on to use his phone's reader, he may also receive spam from other advertisers to whom he has not given consent, such as a text message from another advertiser that has an RFID-reader nearby and has detected the mobile phone user's presence by reading the RFID tag in his phone. To generate a spam message, the other advertiser would also need access to enough personally-identifying information about the phone user in order to send the m-ad without any action on the part of the phone user. If the mobile phone user's RFID-tag includes his mobile phone number or if it simply includes a unique identifying number that can be used to access a database containing his mobile phone number, the rival advertiser will be able to send an m-ad to the mobile phone user.[118]

---

115. *See* Holson, *supra* note 33 (reporting on the increase in mobile spam and efforts by telecommunications carriers and companies producing spam detecting software to detect and block mobile spam).

116. *See supra* Exhibit A.

117. *See infra* Part VII for a discussion of the legal regulations on sending spam messages in the United States and European Union, including requirements to obtain consent to send mobile advertising.

118. *See* Press Release, Fed. Trade Comm'n, The Truth About Cell Phones and the Do Not Call Registry: Despite Re-Circulating E-mail, It Is Still Not Necessary to Register Cell Phone Numbers (June 21, 2006), *available at* http://www.ftc.gov/opa/2006/06/dnccellphones.shtm. The National Do Not Call Registry accepts registrations from both cell phones and land lines. *See* King, *supra* note 27, at 276. In the United States, there is no federal law that precludes mobile carriers from disclosing consumers' mobile phone numbers for the creation of directories; however, there are no official mobile phone directories published by telephone companies. *Id.* at 326. Furthermore, it is generally lawful for unofficial directories to be created by data banks or by businesses for the purpose of delivering m-ads. *Id.* However, there are unofficial directories of cell phone numbers. *See, e.g.*, Cell Phone Numbers, CellPhoneNumbers.com, http://www.cellphonenumbers.com/ (last visited Jan. 4, 2009) (reporting on the best cell phone directory sites, which include 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). *Id.* However, in Janu-

Second, the risk that the user of an RIFD-equipped mobile phone may inadvertently download adware or spyware is a more significant privacy concern.[119] Having an RFID-reader in a mobile phone creates a new way for adware and spyware to be downloaded to a phone.[120] Consider a scenario in which a mobile phone user uses their RFID-reader to access a smart poster in order to obtain a travel guide for a city that she is visiting. Along with downloading the top ten sights to see in Paris, a software program is downloaded to the user's phone that will generate m-advertising, such as pop-up ads for local stores or restaurants. Or perhaps the downloaded software is actually designed to communicate the user's mobile phone number to an advertiser so that it can send m-ads as text or multi-media messages. Once adware or spyware software is stored in the memory of a mobile phone, it can be used to deliver advertising on the mobile phone and engage in other privacy-invasive behavior (such as communicating the user's contact list or passwords stored on the phone to an outside party without notice or consent) in ways that are analogous to the risks of adware and spyware downloads from the Internet to desktop or laptop computers.[121]

D. *Tracking*

If the information stored on an RFID-tagged consumer item is unique to the particular item, it can be used to distinguish the person carrying the item from all other persons and thus be used to track the person carrying the RFID-tagged item.[122] "Tracking is enabled by the collection or processing of location and time data and can be performed either after

---

ary 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* Peter Svensson, *Database Company Intelius Shuts Down Cell-phone Directory After Consumer Complaints*, NWI.COM, Feb. 6, 2008, http://nwitimes.com/articles/2008/02/06/business/business/doce3e5fa64e896806b862573e5007c210f.txt.

119. For a discussion of the legal restrictions on deploying spyware and adware in the United States and the European Union, *see infra* Part VI.

120. *See* Garrie & Wong, *supra* note 31, at 481 (discussing the need to broaden the term "parasiteware" to include unauthorized forms of spyware that accompany cell-phone applications).

121. *Id.*

122. *OECD Report on RFID*, *supra* note 16, at 39 ("[T]racking people is possible if they carry or wear objects that include RFID tags.").

the fact with data already stored in a database, or in real time."[123] It is important to consider the privacy implications regarding the uses by consumers of RFID-tagged mobile phones that could enable others to track and distinguish users through an RFID-enabled mobile phone.

After-the-fact tracking can be produced by RFID systems by bringing together location, time and other information, which has been previously stored in one or more databases, a process that has been called production of "digital footprints."[124] For example, initial tracking of an RFID-tagged ticket of an identified or unidentified sporting fan for access control to a sporting event could be followed by later processing to reveal information about the participant's activities and behavior at that event, such as which concessions he purchased. In contrast, real-time tracking using RFID-tags enables the tracker to distinguish an individual in a group and to monitor his behavior while it is occurring, even when the tracker does not know the person's identity.[125] To do so, the monitor needs to provide the individuals with functional tags (not blocked or deactivated) that can later be read and to place readers at appropriate locations, taking into consideration the operation ranges of RFID technologies.[126]

The interoperability of the RFID tags is also relevant to tracking. This issue relates to whether parties other than the party that originally supplied the RFID-tagged item are able to read the tag.[127] The OECD has limited its discussion of tracking using RFID by expressly excluding the privacy implications of open infrastructure that could be used for tracking objects and people.[128] However, the emerging context of RFID-enabled phones in RFID-embedded environments, as illustrated by ongoing consumer trials of RFID-enabled phones, will force this discussion. The BART RFID trial demonstrates the efforts of industry groups like Near Field Communication Forum to develop technology that will permit interoperability of RFID-tagged items and systems.[129]

---

123. *Id.* at 40. Tracking individuals is possible even though no personal data are stored in an RFID tag carried by the individual. Personal information about the individual may be obtained thereafter when the person uses his or her credit card, bank card, shopper card, etc. The "link between the unique RFID number of the tag and a person's identity needs to be made only once for the card to serve as a proxy for the person thereafter." Albrecht, *supra* note 7, at 75.

124. *OECD Report on RFID*, *supra* note 16, at 39.

125. *Id.* at 40.

126. *Id.*

127. *Id.*

128. *Id.*

129. *See* discussion of the BART RFID Trial, *supra* Part III.

E. *Profiling*

Profiling is "a computerized method involving data mining from data warehouses, which makes it possible, or should make it possible, to place individuals, with a certain degree of probability, and hence with a certain induced error rate, in a particular category in order to take individual decisions relating to them."[130] Sophisticated machine profiling by businesses engaged in customer relationship management (CRM) is designed to gather "relevant data about as many (potential) customers as possible as part of marketing and sales strategies [in order to use that data to try to determine] which customers may be persuaded to become their new customers under what conditions."[131] The delivery of LBS and m-advertising are applications of personalized marketing and CRM that focus on delivering location and time relevant services and advertising to customers and potential customers. To the extent that delivery of LBS and m-advertising uses automated profiling in this process, it needs to be analyzed for its impact on consumer privacy.

Profiling is accomplished by machines that are "software programs trained to recover unexpected correlations in masses of data aggregated in large databases."[132] The profiling process does not merely query the database to find data that is already known to be there, such as the sum of attributes already recorded in the database; rather it attempts to "discover knowledge" that was not already known to be in the data.[133] The

---

130. Dinant et al., *supra* note 13, at 5.

131. Hildebrandt, *supra* note 65, at 2 (alteration in original). *See also* Dinant et al., *supra* note 13, at 9–10 (discussing applications of data mining for personalized marketing and customer relationship management and marketing).

132. Hildebrandt, *supra* note 65, at 5.

133. *Id.* According to Hildebrandt:

> Automated profiling can be described as the process of knowledge discovery in databases (KDD), of which data mining (DM; using mathematical techniques to detect relevant patterns), is a part. KDD is generally thought to consist of a number of steps:
>
> (1) recording of data
>
> (2) aggregation & tracking of data
>
> (3) identification of patterns in data (DM)
>
> (4) interpretation of outcome
>
> (5) monitoring data to check the outcome (testing)
>
> (6) applying the profiles

Id. (citations omitted). This type of profiling is new in two ways: it is produced by machines and it differs from classical empirical statistics because it results from a hypothesis that emerges in the process of data mining that is then tested on the population rather than a

major privacy concern regarding profiling used for CRM purposes, such as facilitating targeted marketing to support delivery of LBS and m-advertising, is that it may result in "asymmetry of access to knowledge" between customers and marketers.[134] The harm from this asymmetry of knowledge is that a customer who is "unaware of the profiles that are applied to her . . . may be induced to act in ways she would not have chosen otherwise."[135] Mireille Hildebrandt gives the example of a person whose online behavior is profiled and matched with a group profile that predicts that the chance that she is a smoker on the verge of quitting is 67 percent.[136] A second profile also predicts that if she is offered free cigarettes together with her online groceries and receives news items about the reduction of dementia in the case of smoking, she has an 80 percent chance of not quitting.[137] If a tobacco company generates the profiles described above for marketing purposes, the customer's behavior may be influenced, thereby inducing her to purchase cigarettes, yet she will be unaware of the group profiles used to target her as a potential customer by the marketer. From a privacy analysis, the customer cannot exercise her personal autonomy to the extent that she is unaware of the knowledge produced and used by the profiling practices of the marketer.[138] Protection of her privacy interest in this regard calls for providing a regulatory mechanism that will protect her autonomy in the sense of enabling her to gain access to the knowledge profiles that are being used by marketers to select her for particular types of ads and promotions.[139] Presumably, if she has the same information as the marketers about the knowledge profiles she falls in, she may choose to exercise her autonomy and change her behavior, such as resisting the

---

sample. *Id.* at 6. An advantage of KDD is that it can "trace and track correlations in an ever-growing mass of retained data and confront us with inferences drawn from past behavior that would otherwise be lost to oblivion." *Id.* (citations omitted).

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

135. *Id.* at 9.

136. *Id.* at 9–10.

137. *Id.* at 10.

138. *Id.*

139. *Id.* at 10–12, 15–17 (arguing for regulation that creates a privacy right to access, in real-time, knowledge profiles being applied to people; including the potential consequences, in order to protect personal autonomy). Hildebrandt argues that Transparency-Enhancing Technologies (TETs), as well as Privacy-Enhancing Technologies (PETs), need to be provided with respect to the use of the smart technologies that enable Ambient Intelligent (AmI) Environments, and she lists sensor technologies, RFID systems, nanotechnology and miniaturization as the enabling technologies. *Id.* at 7, 15–17. The use of Transparency-Enhancing Technologies to protect privacy is discussed *infra* Part V.A.

free cigarettes or seeking treatment to stop-smoking. The important benefit of making the profiles transparent to the customer is that she is then empowered to acquire knowledge of the profiles and this awareness will enable her to avoid being unfairly manipulated.

However, automated profiling does not always utilize personally-identifying data about individuals. To the extent that profiling processes use personally-identifying information about individuals, the data protection concerns discussed earlier in this section are applicable.[140] However, when profiling is based on anonymous data or the application of group profiles to an anonymous person, the process does not necessarily involve processing personal data.[141] To the extent that profiling practices do not collect or make use of personally identifying information about the individuals profiled, existing data protection laws may not

---

140. *See supra* Part IV.A. *See also* Dinant et al., *supra* note 13, at 12–14 (discussing application of Article 15 of the European Union's Data Protection Directive to render the making of automated decisions about individuals a data protection violation in some circumstances). However, the European Union's Data Protection Directive's applicability depends on all four of the following conditions being met:

> -a decision must have been taken;
>
> -this decision must have legal effects in respect of a person or affect him/her significantly;
>
> -the decision must have been taken solely on the basis of automated data processing; [and]
>
> -the data processed must be designed to evaluate certain personal aspects of the individual affected by the decision.

Id. at 14. The CRID Profiling Study comments that sending a brochure to a list of people selected on the basis of automated processing cannot be considered as significantly affecting the person within the meaning of Article 15, but

> [O]ther types of advertising used in cybermarketing seem more problematical, particularly when they involve unfair discrimination based on an analysis of clickstream data (for example, a person visiting a Web site who is offered goods or services at a higher price than others, or a person who is refused the opportunity to purchase goods or services that are available to others).

Id. at 13–14. The CRID Profiling Study discusses the possibility that Article 15 "could cover the development of a profile derived from data which are not necessarily and directly personal within the meaning of the relevant legislation," since Article 15 regulates a type of decision (automated decisions) and not just the processing of personal data, providing the other conditions are met. *Id.* at 14.

141. Data protection law only protects personal data of identifiable persons, while most profiling is done on the basis of anonymized data to which the legislation does not apply. Wim Schreurs et al., *Legal Issues: Report on the Actual and Possible Profiling Techniques in the Field of Ambient Intelligence*, FIDIS DELIVERABLE 7.3, 48–49 (2005) (on file with author), *available at* www.fidis.net. In the same way, the application of a group profile to an anonymous person does not fall within the scope of data protection legislation, although it may have substantial consequences for this person. *Id.*

apply.[142] Thus, these business practices mainly give rise to broader concerns of personal privacy, rather than data protection concerns.

The advent of RFID-enabled phones to be used by consumers in RFID-embedded environments designed for LBS and m-advertising purposes will generate a great deal of data about consumers' locations, purchasing habits and other details of their daily lives. This will fuel automatic profiling systems designed to produce knowledge about consumers for marketing purposes. The consumer data generated from this new context can be collected and stored as anonymous data in data warehouses that also store data collected from other sources. Data mining would then be applied to the data in the warehouse to identify correlations between groups of consumers and to produce group profiles to be used for marketing purposes. Ultimately, a particular consumer would be included in a group profile and the particular ads, promotions and other communications he receives would be based on this classification. Yet, without disclosure of the profiles that are being applied to the consumer, the consumer would not know why he is not treated the same as consumers in other classifications that, for example, may receive more favorable promotional opportunities from a marketer.

V. Self-Regulatory Tools to Protect Privacy and Personal Data

Technologies to enhance privacy and the use of protective privacy policies are two of the key self-regulatory tools aimed at protecting consumers' privacy and personal data. Both will be explored in this section.

A. *Privacy-Enhancing Technologies*

Privacy-Enhancing Technologies (PETs) encompass "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."[143] The advantage of PETs is that they may offer those in mobile commerce anonymity and enable the consumer to participate without revealing his or her identity or otherwise providing

142. Use of anonymous data for profiling purposes may satisfy data protection rights under Council of Europe Convention 108 and the Data Protection Directive, but it does not eliminate the individual's privacy rights under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Dinant et al., *supra* note 13, at 30–31. *See also* Hildebrandt, *supra* note 65, at 12–14 (discussing applications of profiling to customer relationship management and marketing).

143. Solove et al., Information Privacy Law 1, 624 (2d ed. 2006) (internal quotations omitted).

personally identifying information (PII).[144] A second potential technological solution, Platform for Privacy Preferences ("P3P"), has also been proposed to protect consumer privacy in e-commerce.[145] P3P is software designed to monitor Web site privacy policies. It enables consumers to communicate their privacy preferences before the Web sites they visit are able to collect their PII. Then, consumers are able to make choices about whether to visit the Web sites and, if so, to provide their PII.[146] P3P is currently underutilized "due to a lack of significant customer and industry buy-in."[147] 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.[148]

Making a distinction between Transparency Enhancing Technologies (TETs) and the broader concept of PETs helps focus consumer privacy discussions related to AmI technologies on the question of whether it is transparency, rather than anonymity, that consumers most need in the context of emerging uses of RFID systems and other AmI technologies.[149] For example, when customer relationship management use computer profiling to provide targeted services to customers, Mireille Hildebrandt argues that providing adequate transparency means giving consumers access to the profiles that are being applied to them so that they have the opportunity to assess the impact of profiling on their lives.[150] Furthermore, because RFID systems produce "an immense

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

145. SOLOVE ET AL., *supra* note 143, at 642. *See also* Ciocchetti, *supra* note 101, at 97.

146. Ciocchetti, *supra* note 101, at 97.

147. *Id.*

148. Evelyne Beatrix Cleff, *Implementing the Legal Criteria of Meaningful Consent in the Concept of Mobile Advertising*, 3 COMPUTER L. & SEC. REP. 262, 267–68 (2007) (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).

149. Hildebrandt, *supra* note 65, at 16–17. *See generally* PROFILING THE EUROPEAN CITIZEN, CROSS–DISCIPLINARY PERSPECTIVES (Mireille Hildebrandt & Serge Gutwirth eds., Springer 2008).

150. Hildebrandt, *supra* note 65, at 2–3, 9–11, 12–13, 17 (providing an example of the types of profiles that could be applied by a tobacco company to target customers likely to engage in purchasing behavior that is profitable to the company and explaining why consumers need access to information about the profiles being applied to them in contexts like this).

amount of data about (change of) location and if linked to other data they provide a rich resource for profiling practices," there is a special need for TETs in RFID applications.[151] While PETs that are designed to protect consumer privacy will naturally focus on hiding data and on the use of pseudonyms that will enable consumers to be anonymous in the presence of RFID technologies, these types of technological protections for privacy will not be adequate to minimize the privacy risks associated with autonomic profiling because consumers will need more than just the ability to avoid identification.[152] Instead, what consumers need to protect their privacy in a world of autonomic computing is access to the profiles that are used with respect to them, which means that effective TETs must be put into place.[153] In this regard, Mireille Hildebrandt argues that the present generation of data protection laws fail as privacy regulation largely because they do not address the real privacy issue, which is the generation of highly sophisticated group profiles that are applied in ways that significantly impact the privacy of those profiled:

> To counter the threats of autonomic profiling citizens will need more than the possibility of opting out, they will need effective transparency enhancing tools (TETs) that render accessible and assessable the profiles that may affect their life . . . . [W]e urgently need to develop transparency-enhancing tools to match the proactive dimension of our smart environments. This will require substantial cooperation between social scientists, computer engineers, lawyers and policy makers with a clear understanding of what is at stake in terms of democracy and the rules of law.[154]

B. *Privacy Policies*

Privacy policies are 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' personally identifying information.[155] In other words, privacy policies give notice or disclose an organization's privacy practices to individuals who are on the receiving end of m-advertising. The extent to which a company-specific privacy policy complies with fair information principles advocated or adopted by various organizations is a measure of

---

151. *Id.* at 15–17.
152. *Id.*
153. *Id.*
154. *Id.* at 17.
155. Ciocchetti, *supra* note 101, at 68.

how well that policy is designed to protect the personal data and privacy of individuals.

There is a growing consensus among privacy experts that complex privacy policies contained in a single document are not an effective way to communicate with consumers about the fair information processing practices of a business.[156] 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.[157] According to privacy experts, whether the notice is provided online or in paper form, a short initial privacy notice should be provided to the consumer that discloses:

(1) Who is covered by the privacy notice (i.e., who is the responsible person or entity);

(2) The types of information collected directly from the individual and from others about the individual;

(3) Uses or purposes for the data processing;

(4) The types of entities that may receive the information (if it is shared);

(5) Information on choices available to the individual to limit the use and/or exercise of any access or other rights, and how to exercise those rights; and

(6) How to contact the data collector for more information and how to complain (to the collector and to an independent oversight body, if appropriate).[158]

In determining whether a privacy policy conveys appropriate notice of a company's privacy practices, it is important to look at the nature of the medium on which the privacy policy and disclosures about the policy

156. *See id.* at 101 (arguing the "future of electronic privacy policies lies in a multilayered notice format rather than one long and complex document."). *See also* CTR. FOR INFORMATION POLICY LEADERSHIP, TEN STEPS TO DEVELOP A MULTILAYERED PRIVACY NOTICE 1–9 (Mar. 2007), http://www.hunton.com/files/tbl_s47Details %5CFileUpload265% 5C1405%5CTen_Steps_whitepaper.pdf; Martin Abrams et al., Memorandum, Berlin Privacy Notices (Apr. 2004), http://www.hunton.com/files/tbl_s47Details/FileUpload265/681/Berlin_ Workshop_Memorandum_4.04.pdf.

157. *See* references cited *id.*

158. *See* Abrams et al., *supra* note 156 (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 are the initial notices contemplated under this multilayered privacy approach, the additional completed notices would include all the details required by relevant laws. *Id.*

are made and on which the consumer will convey her consent. Currently, the viewing screen on most mobile phones is very small. Although some screens are getting larger, they are likely to remain very small compared to the screen on a desktop or laptop computer. The possibility of using multilayered privacy policies, as opposed to a comprehensive stand-alone privacy policy, is especially relevant in this discussion of obtaining appropriate consent for m-advertising.[159]

Industry associations of global businesses involved in m-advertising are proposing model privacy policies for their members to address privacy and data protection concerns of m-advertising and location-based services. In some cases, when the industry focuses on applications of RFID technologies, these policies may also address specific privacy issues related to their members' use of RFID technologies. 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.[160] The 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.[161] The MMA's Code of Conduct is based on five categories: Notice, Choice & Consent, Customization & Constraint, Security and Enforcement & Accountability.[162]

---

159. *See* Ciocchetti, *supra* note 101, at 101. 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]." *Id.* at 102, fig.1. *See also DMA Policy Generators*, DIRECT MKTG. ASS'N, http://www.the-dma.org/privacy/privacypolicygenerator.shtml (last visited Jan. 4, 2009).

160. *See About the MMA*, MOBILE MARKETING ASSOCIATION, http://mmaglobal.com/ (last visited Jan. 4, 2009). The MMA is headquartered in the United States 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 The Internet of Things*, *supra* note 1, 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.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.*

161. *See About the MMA*, *supra* note 160.

162. *See Code of Conduct for Mobile Marketing*, MOBILE MARKETING ASSOCIATION, http://mmaglobal.com/modules/content/index.php?id=5 (last visited Jan. 4, 2009) [hereinafter *MMA Code of Conduct*].

This code is an exercise of industry self-regulation that has a highly pro-consumer privacy aim:

> 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.[163]

On a regional level, the Federation of European Direct Marketing (FEDMA) has also adopted a code of conduct for its members.[164]

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 indirectly, 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.[165] 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).[166] 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. In addition, the Spam Code is only mandatory for those members who have signed it.[167] However, in the context of mobile spam, it does require member operators who are

---

163. *The Internet of Things*, *supra* note 1, at 93.

164. The European Commission recently issued Communication on Data Protection and notes that its Article 29 Working Party approved policy was established by FEDMA and characterizes it as an important milestone in self-regulation. *See Communication from the Commission to the European Parliament and the Council on the Follow-Up of the Work Programme for Better Implementation of the Data Protection Directive*, COM (2007) 5 final, (Mar. 7, 2007), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/com_2007_87_f_en.pdf [hereinafter EC Communication on Data Protection].

165. *About GSM Association*, GSM WORLD, http://www.gsmworld.com/about-us/index.htm 9 (last visited Jan. 4, 2009).

166. *GSM Association Mobile Spam Code of Practice*, GSM WORLD, (Feb. 2006), http://www.gsmworld.com/documents/mobile_spam.pdf. This code "takes a firm stance on how to deal with mobile spam messages that are either fraudulent or unsolicited commercial messages." *Id.*

167. *Id.*

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."[168]

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.[169] 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.[170] Of all the industry associations engaged in examining how consumer privacy impacts their business practices, the NFC Forum is the one best situated to address the privacy issues related to the use of RFID-enabled phones for delivery of LBS and mobile advertising. This is because its members represent all of the kinds of businesses that will be involved in using RFID technologies for LBS and mobile advertising purposes, including global telecommunications carriers, application providers and mobile handset manufacturers.[171] Yet, as demonstrated by the large number of businesses that are working together in the BART RFID Trial, it will likely be very difficult for its members to agree on an industry privacy code to protect consumers, even without considering the global nature of its membership that often operates under different regulatory frameworks. The NFC's Privacy Advisory Council has not adopted a privacy code of conduct for its members and has not announced a plan to adopt such a code, although it has said it is planning to issue a position paper that addresses policies for the protection of privacy when using NFC technology as well as a checklist to ensure interested parties are aware of each of the privacy tenets.[172]

---

168. *Id.*

169. *See* Near Field Communication (NFC) Forum, http://nfc-forum.org/home (last visited Jan. 4, 2009) (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.").

170. *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), http://www.nfc-forum.org/resources/white_papers/nfc_forum_marketing_white_paper.pdf.

171. *See* Near Field Communication (NFC) Forum, http://www.nfc-forum.org/member_companies/ (last visited Jan. 4, 2009) (discussing membership of the NFC Forum). *See also* discussion of focus on NFC technologies in the BART RFID Trial, *supra* notes 67, 71.

172. *See* Near Field Communication (NFC) Forum, Committees and Working Groups, http://www.nfc-forum.org/aboutus/committees_and_wgs#pac (last visited Jan. 4, 2009). In contexts that do not address the use of RFID in mobile phone handsets or embedding con-

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 how to practically implement the theory to provide fair information practices for consumers.[173] 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, but consumers assume that such policies do protect their privacy and personal data.[174] Critics also argue that companies recognize that consumers do not read or understand paper or electronic privacy policies.[175] 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 by including privacy disclaimers that enable the companies to do as they will with consumers' PII, even to the point of selling consumers' personal data to third parties.[176] To the extent 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

---

sumer environments with RFID technologies for the delivery of LBS and mobile advertising, some industry codes and nonprofit organizations have issued guidelines to address privacy issues related to RFID. *See, e.g.*, *European Policy Outlook RFID*, FEDERAL MINISTRY OF ECONOMICS AND TECHNOLOGY, 30 (2007), http://www.nextgenerationmedia.de/documents/European_Policy_Outlook_final_version.pdf (reporting that EPC global has issued binding guidelines for all its members that requires labeling of products containing RFID, extensive consumer information and the possibility to deactivate RFID tags at the points of sale; major retailers in the United Kingdom have agreed upon a code of conduct for the implementation of RFID in the retail sector; and the International Chamber of Commerce and the United States' Center for Democracy and Technology have created guidelines for the application of RFID in the area of the end consumer). *See also Guidelines on Commercial Use of RFID Technology*, EPIC (2004), http://epic.org/privacy/rfid/rfid_gdlnes-070904.pdf [hereinafter *EPIC's Guidelines on Commercial Use of RFID Technology*].

173. *See, e.g.*, Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN ST. L. REV. 587, 610–11 (2007) (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). *See also* references for privacy guidelines designed to address the use of RFID technologies, *id.*

174. *See id.* at 611 (reporting on a survey that found 75 percent of consumers believed their information could not be sold just because a Web site has a privacy policy and another survey that found 57 percent believed that the mere presence of a privacy policy meant the Web site could not share consumers' personal information with third parties).

175. *See* Ciocchetti, *supra* note 101, at 69–70 (reporting that studies show Web site visitors are not 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).

176. *See id.* at 69.

enforcement of the standards—they generally have failed to ensure fair information practices that protect consumers.

Of course, government regulation is also an important tool to protect consumers' privacy and data protection. This article now compares the existing regulatory frameworks in the European Union and the United States to examine how the law in these regions answers significant privacy and data protection questions arising from m-commerce contexts that include RFID-equipped mobile phones, LBS, and accompanying m-advertising.

VI. E.U. AND U.S. REGULATORY FRAMEWORKS FOR RFID APPLICATIONS

In both the United States and the European Union, efforts to regulate RFID take place in a legal framework that heavily regulates providers of mobile communications services[177] and generally prohibits unfair commercial practices.[178] The European Union's Unfair Commercial Practices

177. Under the European Union's regulatory framework, information society services (including mobile and wireless communication services) are the responsibility of the Information Society and Media Directorate General, one of the Directorates General that make up the European Commission. *See* Information Society and Media Directorate General, European Commission, *available at* http://ec.europa.eu/dgs/information_society/index_en.htm (last visited Jan. 2, 2009). Mobile phone devices and mobile communication services are regulated as information society services. *See* Thematic Portal, Information Society and Media Directorate, European Commission, http://ec.europa.eu/information_society/index_en.htm (last visited Jan. 2, 2009). Furthermore, regulation of e-commerce is generally addressed as regulation of information society services. *See, e.g.*, Directive of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular e-Commerce, in the Internal Market, 2000/31/EC, pmbl. 7–8 O.J. (L 178) 1 (EU), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF [hereinafter E-Commerce Directive]. The E-Commerce Directive requires that specified types of information be included in promotional offers and that required information be clear. *Id.* art. 6. Advertisements, including m-ads, must be identifiable to the consumer as commercial communications. *Id.* arts. 6(a), 7. It is illegal to disguise the sender's identity in a commercial communication. *See infra* Part VII.B. for a discussion of the U.S. Federal Communication Commission's regulatory powers over providers of mobile and wireless communications services and the U.S. Federal Trade Commission's powers to protect consumers from unfair or deceptive trade practices related to advertising.

178. Council Directive 2005/29/EC, O.J. (L 149) 22 (EU), *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_149/l_14920050611en00220039.pdf [hereinafter *Unfair Commercial Practices Directive*]; 15 U.S.C. § 57a(a)(1)(b) (2008) (providing FTC enforcement authority that covers unfair or deceptive acts or practices that occur in or affect interstate commerce). The Federal Trade Commission Act (FTC Act) in the United States generally prohibits unfair or deceptive trade practices. *Id.* § 57a(a)(1)(b). The U.S. law allows states to adopt laws that are more protective of consumers than the federal law. *See, e.g.*, discussion of state consumer protection laws that exceed the federal consumer protection laws regarding restrictions of telemarketing practices. FTC, Comments of Verizon Wireless *in re* Telemarketing Sales Rules Review, FTC File No. P994414, (Fed. Trade Comm'n May 16,

Directive, which must be implemented into Member-States' laws and allows Member-States to adopt national laws that provide additional health and safety protections for consumers, is similar to the Federal Trade Commission Act in the United States (FTC Act), as both laws apply to unfair and deceptive marketing practices.[179] But unlike the FTC Act, the European Union's Unfair Commercial Practices Directive is more specific in its definitions of prohibited business practices.[180] Both the U.S. and E.U. laws prohibiting unfair or deceptive commercial practices may help curb abusive marketing practices, including those of companies that adopt privacy policies as self-regulatory tools, but then fail to live up to those policies.[181]

The applicable law in the European Union and United States which protects consumers from privacy risks related to data protection, tracking, spamming, skimming, eavesdropping and profiling is discussed in the next section, including identification of gaps in the regulation. This is followed by a comparison of the differences and similarities in the two regulatory frameworks.

A. *European Union Regulatory Framework Focuses on Data Protection*

The starting point for understanding the E.U. privacy law is a recognition that privacy legislation is primarily about protecting individuals' personal data from unauthorized processing. In the European Union, individuals have personal data protection under treaties and other legislation.[182] The Data Protection Directive (95/46/EC) requires E.U.

2006), *available at* http://www.ftc.gov/bcp/rulemaking/tsr/comments/verizon.htm [hereinafter Verizon Comments on the TSR].

179. *Compare* 15 U.S.C. § 57a(a)(1)(b) (2008) (providing FTC enforcement authority that covers unfair or deceptive acts or practices that occur in or affect interstate commerce) *with Unfair Commercial Practices Directive*, *supra* note 178, arts. 3, 11, 19.

180. *See Unfair Commercial Practices Directive*, *supra* note 178, arts. 6 (defining misleading actions), 7 (defining misleading omissions), 8 (defining aggressive commercial practices), 9 (prohibiting use of harassment, coercion and undue influence).

181. See Agreement Containing Consent Order, Gateway Learning Corp., File No. 042-3047 (Fed. Trade Comm'n 2003), *available at* http://www.ftc.gov/os/caselist/0423047/040707agree0423047.pdf, for an example of a FTC enforcement action against a company that violated its own privacy policy. *See also* 15 U.S.C. § 57a(a)(1)(b); *Unfair Commercial Practices Directive*, *supra* note 178, art. 6(2)(b) (prohibiting as a misleading action the non-compliance with commitments capable of being verified (not merely aspirational) that have been made by a business in a code of conduct to which the business has agreed to be bound); Ciocchetti, *supra* note 101, at 72–74. The situation of businesses adopting privacy policies but failing to follow them has been identified as an example of the weakness in relying on industry self-regulation to protect consumers' privacy and personal data and the need for government regulation. *See supra* notes 173–176, 180 and accompanying text.

182. *See* Treaty of Amsterdam Amending the Treaty on European Union, the Treaties Establishing the European Communities and Related Acts, 1997 O.J. (C 340) 2 (Nov.

Member-States to adopt data protection legislation regulating the processing of personal data and the free movement of such data.[183] This Directive expressly refers to the fundamental rights of privacy that are contained in conventions and treaties and states the intention to regulate the processing of personal data consistent with these fundamental rights.[184] In 2002, the E-Privacy Directive was adopted to regulate the processing of personal data in the electronic communication sector, which includes publicly-available telecommunications and Internet services.[185] The Data Protection Directive is general legislation that provides the principles of data protection for natural persons in the European Union and it is supplemented by the more specific E-Privacy Directive that covers the electronic communications sector.[186] While the Data Protection Directive applies to all processors of personal data, the E-Privacy Directive applies only to publicly available electronic communications services in public communications networks in the European Community (hereinafter "public carriers").[187] Therefore, data processing that uses the services of mobile carriers and public Internet service providers is covered by the E-Privacy Directive as well as the Data Protection Directive, but data processing by other businesses, such as m-advertising

---

10, 1997), *available at* http://eur-lex.europa.eu/en/treaties/dat/11997E/htm/11997E.html #0173010078 (recognizing the Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and requiring Members of the European Union to respect the fundamental rights guaranteed by the Convention). 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 (2000) [hereinafter E.U. Charter].

183. *Data Protection Directive*, *supra* note 97, art. 4.

184. *Id.* at pmbl. (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 European Union. *See, e.g.*, International Covenant on Civil and Political Rights and Optional Protocol to the International Covenant on Civil and Political Rights, G.A. Res. 2200 (XXI), U.N. GAOR, 21st Sess., Supp. No. 16, U.N. Doc. A/6316 (1966) [hereinafter ICCPR].

185. Council Directive 2002/58/EC, art. 1, 2002 O.J. (L 201) 37 (EU), *available at* http://mineco.fgov.be/internet_observatory/pdf/legislation/directive_2002_58_en.pdf [hereinafter E-Privacy Directive].

186. Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the Follow-Up of the Work Programme for Better Implementation of the Data Protection Directive 2007/C 255/01, ¶ 19, 2007 O.J. (C 255), 1 (EU), *available at* http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-07-25_Dir95-46_EN.pdf [hereinafter EDPS Opinion on Data Protection]. The E-Privacy Directive harmonizes the provisions of Member-States' laws with respect to processing personal data in the electronic communications sector. *Id.* art.1.

187. E-Privacy Directive, *supra* note 185, art. 3(1).

application providers and LBS providers that do not use the services of a public carrier, is only covered by the Data Protection Directive.

The Data Protection Directive applies only to the processing of personal data and limits its scope by defining personal data as information relating to an identified or identifiable natural person.[188] It defines the processing of personal data broadly as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, . . . use, . . . dissemination, [etc]."[189] Individuals ("data subjects") are assured certain rights with respect to their personal data while "data controllers" are required to follow rules and restrictions with respect to their data processing operations, including disclosing to data subjects the identity of any data controller and the purposes for which personal data are being collected.[190] The Data Protection Directive includes core principles of data privacy protection that define the rights of individual data subjects and the responsibilities of data controllers in the context of processing personal data, regardless of the context (consumer, employment, etc.). Pursuant to the Data Protection Directive, personal data may only be collected for specified, explicit and legitimate purposes and may not be processed inconsistently with those purposes (commonly referred to as the "finality principle").[191] The purpose of the processing itself must be legitimate ("legitimacy principle"),[192] and the data subject must be fully informed on the details of the processing, including who has access to the data, how it is stored and how the subject can review it ("transparency principle").[193] The "proportionality principle" requires that personal data be adequate, relevant and not excessive in relation to the purposes for which it is collected and further processed.[194] As a direct and mandatory result of the Data Protection Directive, there are national data protection laws in the E.U. Member-States that are administered by local data protection authorities and

188. *See Data Protection Directive*, *supra* note 97, art. 2(a) (including natural persons "who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"). *But see* Dinant et al., *supra* note 13, at 12–14 (stating that, unlike the other provisions in the Data Protection Directive, Article 15 of this directive, which deals with automated individual decisions, may make it unlawful to make a decision about an individual solely on the basis of automated data processing, even when no personally-identifying information is used in the process, if several cumulative conditions are met).

189. *Data Protection Directive*, *supra* note 97, art. 2(b) (emphasis added).

190. *Id.* art. 10.

191. *Id.* art. 6(1)(b).

192. *Id.* art. 7.

193. *Id.* art. 12.

194. *Id.* art. 6(1)(c).

Member-States' data protection laws have been amended to be consistent with the Data Protection Directive's core principles.[195]

There is ongoing action by the European Commission to further implement the two key E.U. regulatory instruments on data protection: the Data Protection Directive and the E-Privacy Directive.[196] Even without adopting proposed amendments to the E-Privacy Directive that would explicitly mention RFID, there is little doubt that current E.U. law, including treaties and legislation that protect individual privacy and regulate the processing of personal data, also apply to the use of new technologies like RFID.[197] The Article 29 Working Party ("Working Party") recognized early on that important privacy and data protection concerns are involved in the use of RFID technologies, as evidenced by its issuance in 2005 of a working document on data protection issues related to RFID technology.[198] It is clear that the existing data protection

195. *See Data Protection Directive*, *supra* note 97, at 11; *see also* National Data Protection Commissioners, http://ec.europa.eu/justice_home/fsj/privacy/ (last visited Feb. 10, 2009).

196. *See generally Data Protection Directive*, *supra* note 97; E-Privacy Directive, *supra* note 185. *See infra* notes 282–284, 290–296, and 301–304 and accompanying text for discussion of the European Commission's efforts to further implement these two directives.

197. In its Communication on RFID, the European Commission summarized and referenced the applicable treaties that protect personal data in the European Union, including Article 6 of the Treaty on the European Union, which states that the Union is founded on principles of liberty, democracy, and respect for human rights and freedoms, and Article 8 of the Charter of Fundamental Rights, which protects personal data as one of these freedoms. Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, Radio Frequency Identification (RFID) in Europe: Steps Towards a Policy Framework, at 5, COM (2007) 96 final, (Mar. 15, 2007), *available at* http://ec.europa.eu/information_society/policy/rfid/doc/rfid_en.pdf [hereinafter EC Communication on RFID]. It also confirmed that protection of personal data is covered by the Data Protection Directive (*see supra* note 97), regardless of the means and procedures used for data processing and is applicable to all technologies, including RFID. *Id.* at 5–6. ("The protection of personal data is covered by the general Data Protection Directive regardless of the means and procedures used for data processing. The Directive is applicable to all technologies, including RFID."). The European Commission said the E-Privacy Directive (*see supra* note 185) complements the Data Protection Directive, although its applicability is limited to processing of personal data in connection with publicly available electronic communications services in public communications networks. *Id.* at 6. *See also* EC Communication on Data Protection, *supra* note 164, at 7. Describing the Data Protection Directive as technologically neutral, the European Commission commented that "its rules may continue to apply appropriately to new technologies and situations. It may be necessary, though, to translate those general rules into particular guidelines or provisions to take account of the specificities involved in those technologies." *Id.* at 7.

198. The Article 29 Data Protection Working Party: Working Document on Data Protection Issues Related to RFID Technologies, WP 105, 10107/05/EN (Jan. 19, 2005), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf [hereinafter 2005 Art 29 Working Document]. The Article 29 Working Party is an independent European advisory body on data protection and privacy. *Id.* at 1. Its responsibilities are described in Article 30 of the Data Privacy Directive and Article 15 of the E-Privacy Directive. *See Data Protection Directive*, *supra* note 97; E-Privacy Directive, *supra* note 185. The Article 29 Working Party established a subgroup on RFID to analyze the concept of personal data and to

regulatory framework applies to the utilization of RFID technologies in Europe without needing to adopt new legislation or amend existing legislation.[199] However, currently there is no RFID-specific legislation in place in the European Union and neither the Data Protection Directive nor the E-Privacy Directive specifically addresses RFID technologies in the context of consumer privacy and data protection.[200]

Beyond data protection laws, there are other laws in the European Union that apply generally to some of the privacy concerns associated with consumers using RFID-enabled mobile phones to receive mobile advertising and LBS services.

1. Restricting Unsolicited Mobile Advertising

The E-Privacy Directive adopts the data protection principle of "opt-in" notice and consent that requires advertisers to obtain users' consent prior to sending unsolicited advertising messages through publicly available electronic communications services.[201] It specifically covers telemarketing calls made by autodialing equipment and electronic mail.[202] Because the definition of electronic mail in the E-Privacy Directive is broad enough to include mobile advertising sent to a consumer in a text message, voice message, regular e-mail message accessed on the consumer's mobile phone, e-mail delivered on the consumer's mobile phone using a wireless Internet address, and multi-media advertising messages delivered to the consumer's phone, it establishes a general rule that all electronic messages are subject to the requirement that advertisers must obtain the consumer's consent in advance of sending the message.[203] To the extent that mobile advertising uses autodialing equipment or is electronic mail sent using a public carrier, it can only be sent to a consumer on a permissive basis, meaning the consumer must give his consent in advance to receive advertising from the sender ("opt-in" rule), unless covered by an exception to this rule.

There is one important exception to this rule: a person (natural or legal) is allowed to send electronic communications to a consumer in order to directly market the person's own similar products and services to the consumer.[204] The exception only applies if all three of the following

---

address the question of to what extent RFIDs are covered by the Data Protection Directive. *See* EC Communication on RFID, *supra* note 197, at 11 n.19.

199. *See* EC Communication on RFID, *supra* note 197, at 12–18.

200. *See infra* Part VII.A.2 for discussion of the RFID guidelines proposed by the European Commission. *See infra* Part VII.B.1 for discussion of state law efforts to regulate RFID in the United States.

201. E-Privacy Directive, *supra* note 185, art 13(1).

202. *Id.*

203. *Id.* art. 2(h).

204. *Id.* art. 13(2).

conditions are met: (1) the consumer is a customer of the person sending the direct marketing communications; (2) the consumer's electronic contact details were obtained by the person sending the direct marketing from the consumer in the context of a sale of a product or service; and (3) the consumer has the opportunity to object, free of charge, at the time the contact details were collected as well as later, to the sending of direct marketing communications.[205] The E-Privacy Directive prohibits sending electronic mail for direct marketing purposes by "disguising or concealing the identity of the sender on whose behalf the communication is made" or sending electronic mail without a valid address for the consumer to use to send an "opt-out" request.[206]

When advertising is delivered to a consumer on his mobile phone through the phone's RFID reader, must the consumer give advance consent to the advertiser? The E-Privacy Directive does not directly apply in this situation as long a public carrier's network (such as a public telecommunications network or the Internet) is not used in the process of delivering the advertising message to the consumer's mobile phone.[207] As long as the consumer consciously used his RFID reader to access the RFID tag of the advertiser, it seems fair to infer that he has given consent in this situation.[208]

2. Using Location Data to Deliver Mobile Advertising and Other LBS

The E-Privacy Directive defines traffic and location data and is thus part of the regulatory framework for delivering LBS and m-advertising *to the extent that a public carrier is involved*.[209] Public carriers are prohibited from using traffic data for the purposes of marketing electronic communications services or for the provision of value-added services (e.g., location-based services and m-advertising) without the consent of

---

205. *Id.*

206. *Id.* art. 13(4).

207. *Id.* art. 3(1). *See also* EC Communication on RFID, *supra* note 197, at 6 (stating that the applicability of the E-Privacy Directive is limited to "processing of personal data in connection with . . . publicly available electronic communications services in public communications networks.").

208. *See infra* note 376 and accompanying text (explaining how RFID readers read RFID tags in their environment including those that store advertising content). So a consumer's RFID reader may automatically read advertising content from tags in his environment when his phone is brought within proximity to the tags and without a conscious use of the RFID reader for this purpose.

209. Traffic data is "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof". E-Privacy Directive, *supra* note 185, art.2(b). Location data means "any data processed in an electronic communications network, including the geographic position of the terminal equipment of a user of a publicly available electronic communications service." *Id.* art. 2(c).

the subscriber to whom the data relates.[210] Additionally, unless location data has been made anonymous, public carriers must provide specific types of notice to subscribers and obtain their consent before processing location data other than traffic data to provide location-based services or m-advertising.[211] Businesses that are not public carriers also must obtain consumer consent to process location data that is personal data under the Data Protection Directive in order to deliver location-based services and m-advertising, but if they do not use the services of a public carrier, they do not have to comply with the more restrictive rules on using location data found in E-Privacy Directive.[212] This means that in the European Union, using personal data to deliver LBS or m-advertising is not lawful unless it is with the permission of the person receiving the m-ad or other location-based service.[213] However, when RFID-enabled phones and RFID-embedded environments are used to deliver m-advertising, it is not always necessary to involve the services of a public carrier because the communications may occur directly between the consumer's phone and RFID devices embedded in the environment by businesses; thus, currently, the E-Privacy Directive does not apply to this situation.[214] Further, if personal data processing is not involved, for example, if the communications are made without revealing any personally-identifying information about the consumer or being able to link to other sources of

---

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

211. *Id.* art. 9(1). Article 9 also gives subscribers the right to withdraw their consent to the use of location data that is personal data. *Id.* art. 9(1)–(3). Location data:

> May refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel; to the level of accuracy of the location information; to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location was recorded.

Id. pmbl. ¶ 14. Access to location data is essential to providing location-based services through a telecommunications network.

212. *See supra* text accompanying note 185 regarding the scope of the E-Privacy Directive.

213. *See* CONCISE EUROPEAN IT LAW 186–87 (Alfred Büllesbach et al. eds., 2006) ("[A] provider of telephony services could provide location data to a third company in the framework of a processing agreement to provide end customers with weather forecast information or tourist information based on their location data. In such a case, the service provider is required to inform the users and subscribers about the forwarding of their data before they give their consent to the processing of location data other than traffic data for the provision of value added services."); *see also Working Party Opinion on Location Data*, *supra* note 11, at 2–3 (opining that "since location data always relate to an identified or identifiable natural person," they are covered by the Data Protection Directive).

214. *But see infra* text accompanying notes 301–305 (discussing the European Commission's proposal to amend the E-Privacy Directive which, if adopted, will resolve at least part of this regulatory gap).

personal data about the consumer, then generally, the Data Protection Directive does not apply.[215]

3. Restrictions on Spyware and Adware

The E-Privacy Directive prohibits the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of the subscriber or user unless consumers have been given clear and comprehensive information consistent with the Data Protection Directive and the opportunity to refuse processing of their personal data.[216] Terminal equipment is broad enough to include a consumer's mobile phone. The preamble to the E-Privacy Directive specifically mentions spyware:

> Terminal equipment of users' of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.[217]

Thus, the E-Privacy Directive suggests that "any intrusion into the electronic domicile [of the consumer] through spyware, web bugs, hidden identifiers, like cookies or other similar devices, ought to be considered a violation of the private electronic space (virtual domicile), [and] could even be viewed as a form of hacking" punishable as a criminal offense.[218] Accordingly, installing adware is not *per se* illegal, but is subject to the requirements to provide notice and obtain users' consent before downloads can be made to a user's equipment using a public electronic communications network. Consumers have an "opt-out" right to refuse to have a tracking software or devices placed on their mobile

---

215. *See Data Protection Directive*, *supra* note 97. *But see* Dinant et al., *supra* note 13, at 12–14 (discussing application of Article 15 of the E.U. Data Protection Directive to render the making of automated decisions about individuals a data protection violation in some circumstances even when no personal data is used).

216. *But cf.* E-Privacy Directive, *supra* note 185, art. 5(3) (providing exceptions to this rule for technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication or access or as strictly necessary to provide an information society service explicitly requested by the subscriber or user).

217. *Id.* ¶ 24.

218. *See* CONCISE EUROPEAN IT LAW, *supra* note 213, at 169–70.

phones and other terminal equipment.[219] However, spyware, which by definition is deployed without users' knowledge or consent, is illegal if it is downloaded to a mobile phone using a public carrier's network.

4. Prohibitions on Skimming and Eavesdropping

Does the E-Privacy Directive prohibit skimming information from RFID tags in consumers' RFID-enabled mobile phones or interception of radio communications between RFID tags in consumer's mobile phones and RFID readers in a transit mall? The answer is unclear, at least in some circumstances. For example, if the information skimmed is not personal data or linkable to personal data, then generally the Data Protection Directive and the E-Privacy Directive do not apply. It may be that the information obtained by skimming or eavesdropping in the above situations is likely to reveal only a unique identifying number stored on the consumer's RFID tag in his phone that is not linked or linkable to a specific person, and if so, it is not personal data. Furthermore, the skimming of data from an RFID tag by a RFID reader does not necessarily involve the use of an electronic communications network, because such networks are defined in the E-Privacy Directive as "public communications network and publicly available electronic communications services"[220] (public carriers), and it is possible for a person who is not a public carrier and has no relationship to a consumer to place an RFID-reader in a transit mall in order to skim or eavesdrop information. Since this could be done without using a public carrier in any way, arguably the E-Privacy Directive does not apply. However, it is unlikely that skimming or eavesdropping is legal in the European Union, even if the E-Privacy Directive is not applicable. To the extent that personal information is processed by a skimmer or eavesdropper, the Data Protection Directive is still applicable, because its scope is not limited to public carriers. Furthermore, Article 8 of the European Convention for the Protection of Human Rights (ECHR) protects the secrecy of people's correspondence, whether it is in electronic form or not, and irrespective of the technical means of interception or surveillance.

In sum, in the European Union, the primary consumer privacy protections related to RFID-enabled mobile phones used to deliver mobile advertising and other location-based services are primarily a question of data protection. Where RFID-enabled phones are used to deliver m-advertising, there are privacy gaps in the regulation to the extent the services of a public carrier or the use of personal data are not involved. However, even when public carrier services or personal data are not

219. *Id.* at 170 n.5.
220. *See* E-Privacy Directive, *supra* note 185, art. 3(1).

involved, fundamental privacy rights can be expected to apply. Additionally, some Member-States' criminal laws or other more protective civil laws may apply.

B. *U.S. Regulatory Framework for Privacy*

Compared to the framework of general data protection and privacy protections available in the European Union that is acknowledged to cover commercial utilization of RFID technologies for marketing or other purposes,[221] relatively few federal privacy or data protections exist for consumers in the United States.[222] A patchwork of federal laws and two key federal agencies comprise the U.S. privacy and data protection framework. At the federal level, the Federal Communications Commission (FCC) is the key agency responsible for regulating telecommunication carriers and is charged with protecting subscribers from unwanted commercial solicitations on their mobile phones, such as telemarketing and mobile spam.[223] In addition, the FTC, under its powers to enforce laws prohibiting unfair and deceptive trade practices, has the power to bring enforcement actions against businesses who engage in unfair or deceptive trade practices, including those that breach their own privacy policies in their dealings with consumers (even though no law requires businesses to have such privacy policies in the first place).[224]

Federal laws regulating telemarketing and spam and restricting the use by telecommunications' carriers of "customer proprietary network information" can be viewed as providing minimum privacy and data protection standards for m-advertising, although these laws fall far short of providing a comprehensive federal privacy and data protection framework similar to that found in the European Union. This section examines applicable laws in the context of RFID-enabled mobile phones and m-advertising. As this section will show, these laws often have significant gaps in their application to RFID-enabled phones that give rise to privacy and data protection concerns that need to be addressed.

---

221. *See supra* notes 197–199 and accompanying text.

222. The complex nature of U.S. laws that potentially restrict mobile advertising practices and protect consumers' privacy and personal data in this context have been analyzed in depth in a recent study by this author. *See* King, *supra* note 27. Therefore, these laws are discussed only briefly here, to permit this article to focus on the privacy and data protection implications of RFID technologies.

223. *See generally id*. In contrast, this article focuses on applicable federal laws and their potential to address the abuses of mobile advertising directed at RFID-enabled phones.

224. *See id.* at 248 n.30; *see also supra* note 181 and accompanying text.

1. Restrictions on Telemarketing

Under federal law, the making of live unsolicited phone calls for advertising purposes without consumer consent is generally lawful, although consumers have the legal right to "opt-out" of receiving commercial solicitations (e.g., phone calls, text messages or multi-media messages) on their mobile phones by registering their mobile phone numbers on a National Do Not Call Registry or making a request to be placed on a company's own Do Not Call List.[225] Even where consumers have not so opted out, some telemarketing practices are restricted.[226] For example, it is unlawful to make a telemarketing call to a consumer on her mobile phone by using automated dialing equipment without human intervention, unless the consumer has given her advance consent.[227] But if a subscriber is not listed on the Do Not Call List and has not made a specific request to an advertiser to be placed on its company-specific Do Not Call List, it is lawful for advertisers to make live telemarketing calls to consumers on their mobile phones. Constitutionally-based commercial free speech rights limit federal regulation of advertising that is not false and misleading, such that m-advertisers are entitled to some meaningful commercial access to mobile subscribers for commercial advertising purposes.[228] The telemarketing rules do not apply to m-advertising sent

225. *See* King, *supra* note 27, Part V. *See* Rules & Regs. Implementing the Tel. Consumer Prot. Act of 1991, *Rpt. and Order*, 7 F.C.C.R. 8752 (1992); Rules & Regs. Implementing the Tel. Consumer Prot. Act of 1991, *Memorandum Opinion and Order*, 10 F.C.C.R. 12391 (1995); Rules & 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, *Communications Act of 1934—Telephone Consumer Protection Act*, 74 AM. JUR. 2D § 14 (2006). 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)(1)(A)(iii) (2005). *See also* 47 C.F.R. § 64.1200(a)(iii) (2007); 47 C.F.R. § 64.1200(e) (2007) (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 (2007)); *see generally* Rules & Regs. Implementing the Tel. Consumer Prot. Act of 1991, *Rep. & Order*, 18 F.C.C.R. 14014 (2003) [hereinafter 2003 TCPA Order].

226. Phone calls to wireless phone numbers that are *not* live calls are generally prohibited by the TCPA, including calls made using an automatic telephone dialing system. *See* 2003 TCPA Order, *supra* note 225, ¶ 165; *see also* 47 U.S.C. § 227(b)(1)(A)(iii) (2005); 47 C.F.R. § 64.1200(a)(1)(iii) (2007). 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) (2005).

227. *See* 47 U.S.C. § 227(b)(1)(A)(iii) (2005); 47 C.F.R. § 64.1200(a)(1)(iii) (2007); 2003 TCPA Order, *supra* note 225, ¶ 165.

228. *See* Cent. Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 563–64 (1980) (holding that the First Amendment protection of commercial free speech applies to "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.

directly between RFID-enabled devices by wireless contactless communications, as long as the m-ads are communicated to RFID-enabled phones without using regulated telecommunications services. As illustrated by the BART-RFID Trial, the mobile phone user may "read" ads from smart posters that include RFID tags.[229] In this case, the ad is communicated directly from one RFID-enabled device to another and does not use the services of a mobile carrier, so the telemarketing rules will not apply. Since the mobile phone user has initiated the advertising and thus presumably wants to receive the ad, "opt-in" consent rules seem less necessary here and perhaps consent can be implied.

2. Restrictions on Unsolicited Electronic Commercial Communications

Generally speaking, marketers may send unsolicited commercial electronic messages (e.g., unsolicited email advertisements or advertising "spam") to consumers and businesses in the United States without obtaining the advance consent of the recipients as long as: (a) the messages conform to the requirements of the federal spam legislation, Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM) (e.g., not false or deceptive, form requirements met, or "opt-out" notice included); (b) the messages are not sent directly to mobile phone subscribers (Mobile Service Commercial Messages or MSCMs, discussed next); and (c) the recipients have not "opted-out" of receiving these types of commercial electronic messages from the sender.[230] Senders are required to notify recipients that they may elect not to receive future email messages (by making "opt-out" requests to senders) and senders are required to honor recipients' opt-out requests.[231]

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, 736–37 (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).

229. *See* discussion of the BART-RFID Trial, *supra* Part III.

230. 15 U.S.C. § 7704 (2007). *See also* FTC, FTC FACTS FOR BUSINESS: THE CAN-SPAM ACT: REQUIREMENTS FOR COMMERCIAL EMAILERS, (Apr. 2004), *available at* http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm. Consumers also have the ability to "opt-out" from receiving commercial electronic telephone calls (voice or text messages) on their wireless phones by registering their mobile phone numbers on the National Do Not Call Registry. *See supra* Part VI.B.1. Further, some telemarketing practices, such as using autodialing telephone equipment to generate telemarketing calls, are limited by federal law. 15 U.S.C. § 7704 (2007).

231. 15 U.S.C. § 7704 (2007).

CAN-SPAM allows advertisers to send unsolicited email communications to consumers, as long as the consumer has not made a request not to receive such communications, effectively establishing an "opt-out" process of obtaining consumer consent.[232] In contrast, mobile service commercial messages (MSCMs) are a special type of electronic messages that can be sent to mobile phones. To send an MSCM, the sender must obtain the consumer's consent before sending even one message ("opt-in").[233] MSCMs are electronic communications that generally contain advertising messages sent directly to mobile phones via the Internet using a wireless Internet domain name.[234] To ensure that advertisers have the ability to distinguish when an advertising message will be covered by the MSCM rules, the FCC publishes lists of wireless Internet domain names on its Web site.[235] It is possible for anyone with an Internet email account and knowledge of a mobile phone subscriber's mobile telephone number to send an electronic message to the subscriber using a domain name provided by the subscriber's mobile carrier. By sending an email to a mobile subscriber (using the appropriate domain name for the subscriber's mobile carrier and inserting the subscriber's ten digit mobile phone number to create an electronic address for the

---

232. *Id.*

233. 15 U.S.C. § 7712(b)(1) (2009).

234. 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. 15 U.S.C. § 7712 (2009) (emphasis added), 47 U.S.C. § 332(d) (2009). *See also* Lavergne, *supra* note 29, at 886. The term "mobile spam" is often 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 without consent "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 Text Messages and E-Mail on Wireless Phones and Other Mobile Devices, http://www.fcc.gov/cgb/consumerfacts/canspam.html (last visited Jan. 4, 2009). However, if a text message advertisement is generated using automated dialing equipment without the recipient's consent, this would be also be prohibited by the TCPA. *See* 2003 TCPA Order, *supra* note 225, ¶ 165.

235. 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 Jan. 2, 2009) [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 names and to remove any domain names 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 or 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.*

subscriber), the information will be delivered as a text or multimedia message on the subscriber's mobile phone.[236] If CAN-SPAM's restrictive rules did not make it unlawful to send commercial advertising messages in this manner without obtaining 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. 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 express consent.

However, to the extent that it is possible to send mobile advertising messages in the form of pop-up, banner, text messages or e-mail to be accessed by consumers on their RFID-enabled mobile phones without using a wireless Internet domain name on the FCC's published list, the MSCM rules do not apply. When the MSCM rules do not apply, at most, only the "opt-out" notice and consent rules under CAN-SPAM apply.[237] However, under the primary purpose rule, there are situations where CAN-SPAM does not apply to electronic communications sent to mobile devices.[238] If a text message is sent to an RFID-enabled mobile phone, but advertising is not the primary purpose of the communication, the CAN-SPAM will not require opt-out notices to be included. CAN-SPAM would not require opt-out notices for advertising messages sent along with travel information requested by a consumer. Nor would an opt-out notice be required for advertising such as a discount coupon included in a message sent to confirm payment for a purchase made using contactless communications on an RFID-enabled mobile phone. Under CAN-SPAM's primary purpose rule, these promotional messages are likely exempt from most of the form and notice requirements.

---

236. FCC official list, *supra* note 235; Send Email to Phone and SMS Gateways, Email Services, Resources and Tools, http://www.email-unlimited.com/stuff/send-email-to-phone.htm (last visited Jan. 2, 2009). *See* Lavergne, *supra* note 29, at 861.

237. *See* discussion and references, *supra* notes 230–232.

238. 15 U.S.C. § 7702(17) (2007) (exempting transactional or relationship messages that have a primary purpose of facilitating, completing, or confirming a commercial transactions from most of the form and disclosure requirements of CAN-SPAM).

3. Mobile Carriers' Obligations to Protect Subscribers' Personal Data

The FCC also regulates telecommunication carriers' use and disclosure of customer proprietary network information (CPNI), establishing a form of personal data protection for telephone subscribers.[239] The CPNI rules effectively limit the use and disclosure of CPNI for marketing purposes, unless subscribers have given express authorization in advance (essentially requiring opt-in notice and consent for disclosure of this type of personal information by a carrier).[240] However, information that is analogous to that which would be included in a phone directory is not within the definition of CPNI.[241] So, for example, subscribers' mobile phone numbers are not CPNI and there is no law that restricts publication, collection, use, disclosure or even sale of mobile phone numbers, although currently mobile carriers in the United States do not issue official directories of mobile phone numbers.[242]

The CPNI rules are unlikely to provide any real data protection to consumers in the context of RFID-enabled mobile phones except to the extent that mobile carriers are involved in collecting and processing consumers' personal data that is also CPNI. For example, there is the possibility that personal data of mobile phone users with RFID-enabled phones used in RFID-embedded environments will be collected by businesses that are not mobile carriers, such as food retailers and banks that are participating in the BART-RFID Trial. These non-carriers may collect personal data to use for one purpose, like payment of goods and services, but use and/or share the data with other advertisers to generate unsolicited ads. For example, in the BART-RFID Trial, it would be

---

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

240. Section 222(c) of the Telecommunications Act protects consumers' informational 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, except as required by law or with the approval of the customer. 47 U.S.C. § 222(c)(1) (2000). The Telecommunications Act was amended in 1999 to include "location" in the definition of CPNI. Wireless Communications and Public Safety Act of 1999, 47 U.S.C. § 222(h)(1)(A) (1999).

241. *See* 47 U.S.C. § 222(e) (2000) (specifying that notwithstanding the telecommunication carriers' obligations under 47 U.S.C. § 222(b)-(d), the carrier shall provide subscriber list information); 47 U.S.C. § 222(h)(3) (2000) (defining subscriber list information as including information normally included in a phone directory, such as name and address).

242. *See* King, *supra* note 27, at 281–83.

lawful in the United States for consumers' mobile phone numbers, e-mail addresses, purchasing history and other personal data to be stored in a database that is then made available to businesses participating in the trial, thus enabling these businesses to send m-ads by voice or text messages to consumers. Furthermore, because location data only receives CPNI protection when it is generated by using the services of a federally regulated telecommunications carrier, not all location data are protected under U.S. law. It is possible for an advertiser to detect the location of an RFID-tagged mobile phone by placing an RFID-reader in a shopping mall, thus capturing data about the location of the consumer who is carrying the phone, yet this is not the type of location data that is protected as CPNI as it does not relate to provision of mobile phone services by a regulated carrier.[243]

4. Other Potentially Applicable Federal Regulations

Apart from federal laws regulating telemarketing, spam and CPNI that are enforced by the FTC and FCC, the Federal Electronic Communications Privacy Act (ECPA) prohibits interception or unauthorized access to the contents of electronic communications, although there are broad exceptions to this law.[244] The ECPA is discussed here because it may potentially provide some privacy protection for consumers in the context of communications between RFID-enabled mobile phones and RFID readers installed for marketing or other purposes.[245]

Some aspects of applying the ECPA to mobile communications are not yet clear. For example, it is uncertain whether the wiretapping and interception provisions of the ECPA (Title I) apply to interception of call location data related to mobile phone users.[246] In addition, the ECPA's

---

243. *See supra* note 240 and accompanying text.

244. *See* Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522 [hereinafter Title I], 2701–12 [hereinafter Title II], 3117, 3121–27 (2000) [hereinafter Pen Register and Trap and Trace Devices]. Two statutory exceptions exclude from Title I interceptions by "providers of communications systems": (1) the "provider exception," 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."); and (2) the "consent exception," 18 U.S.C. § 2511(2)(c) (2000) (providing that a person "acting under color of law" may intercept an electronic communication if "such person is a party to the communication or one of the parties to the communication has given prior consent to such interception."). *See* 18 U.S.C. § 2511(c) (2000); *see also* SOLOVE ET AL., *supra* note 143, at 269 ("For example a person can secretly tap and record a communication to which that person is a party"). Title II also embraces the provider and consent exceptions. 18 U.S.C. § 2701(c)(1) (2000). *See also* 18 U.S.C. § 2702(b) (2000).

245. *See* Stein, *supra* note 64, ¶ 38.

246. *See* Lee, *supra* note 34, at 395 (explaining that the ECPA grants certain privacy protections to electronic communications under § 2510(12), "[b]ut subsection C explicitly

prohibitions on unauthorized access to stored communications (Title II) must also be examined to determine if they restrict access to location information in computer storage about mobile phone users' locations.[247] 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 could provide some measure of consumer privacy protection.[248]

Even if the ECPA does not protect location data used in providing LBS services, the ECPA may still be important to protect consumers' personal data from unauthorized interceptions and unauthorized access related to information stored on their RFID-enabled mobile phones or communications between their RFID-enabled phones and other RFID-enabled devices. This would be helpful in situations where other federal privacy laws may not apply, such as privacy invasive m-advertising practices by third parties that are not covered by laws regulating telecommunications carriers. For example, if RFID readers are used to "skim"[249] or read personal data on RFID-tags without authorization, such as those embedded in RFID-enabled phones, this could violate Title II of the ECPA, unless one of the exceptions under the law applies. Furthermore, if an unauthorized person "eavesdrops" to intercept data as it is read by an authorized RFID-reader,[250] this could violate Title I of the

---

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.

247. *See* 18 U.S.C. § 2703(c)(2); Lee, *supra* note 34, at 398 (stating that 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 generally* Stored Communications Act (SCA), 18 U.S.C. §§ 2701–2711 (2000). These provisions do not specifically address wireless location information. *See* Lee, *supra* note 34, at 398.

248. *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); *see also* Lee, *supra* note 34, at 396 (suggesting that 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).

249. *EPIC Testimony on AK RFID Bill*, *supra* note 108, at 3.

250. *Id.* at 4. (commenting that "in the absence of effective security techniques, RFID tags are remotely and secretly readable," and that the "creation of a small, easily portable RFID reader may be complex and expensive now, (but) will be easier as time passes"). EPIC's Senior Counsel further testified that the distance necessary to read RFID tags was initially thought to be only a few inches, but tests have shown that RFID tags can be read from thirty to seventy feet away in some instances. Thus, the wireless nature of RFID technology presents a security risk for consumers because they may well be unaware that their personal information has been stolen through skimming or eavesdropping.

ECPA, again provided that one of the exceptions under the law is not applicable.

The Computer Fraud and Abuse Act (CFAA) should also be considered as a possible source of protection for consumers, as related to privacy and security risks associated with RFID technologies, because it prohibits computer fraud and provides a civil remedy for consumers.[251] Arguably it would violate the CFAA for someone to place software on a mobile phone without the phone user's consent for the purpose of generating m-ads.[252]

There is also the possibility that state laws could be adopted or applied by courts to protect the privacy and personal data in the context of LBS and mobile marketing practices involving RFID-enabled mobile phones.[253] Also, state privacy tort laws and state contract laws could be applied to protect consumers' privacy and personal data related to m-advertising and location-based services.[254] However, to date these sources of law, traditionally common law, have provided little privacy and data protection for consumers and have not been used by courts to protect consumer privacy in the context of RFID technologies.

C. *Comparison of E.U. and U.S. Laws*

Generally speaking, E.U. law provides more protection from unsolicited advertising for consumers than U.S. law. For example, E.U. legislation requires Member-States to adopt national laws to curb spam, telemarketing calls and other forms of unsolicited marketing and prohibits sending advertising to consumers unless advertisers have obtained consumers' prior consent.[255] On the other hand, unless consumers have

---

251. 18 U.S.C. § 1030(a)(4) (2008) (providing that whoever "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year" has violated this law); *see also* Garrie & Wong, *supra* note 31, at 493–94 (commenting that the CFAA requires a consumer to prove a loss of an aggregate of five thousand dollars or more in order to recover in a civil action, making it less useful as a tool of redress for consumers in personal data loss situations such as those associated with spyware).

252. 18 U.S.C. § 1030 (2008). *See also* Garrie & Wong, *supra* note 31, at 481 (discussing unauthorized forms of spyware that accompany cell-phone applications).

253. *See supra* Part VII.B for discussion of developments in RFID-specific legislation at the state level and federal and state laws that are designed to protect consumers' privacy in the context of targeted marketing practices that collect and use consumers' personal data for direct marketing purposes.

254. King, *supra* note 27, at 290–301.

255. E-Privacy Directive, *supra* note 185, art. 13. There is an exception to the prior consent requirement that allows the sending of direct marketing of a company's own similar products or services provided that the company gives customers the opportunity to object, free of charge and clearly and distinctly, to the use of electronic contact details when they are col-

"opted-out" of receiving these types of messages, U.S. law generally allows businesses to make live telemarketing calls and to send unsolicited commercial electronic messages to consumers by e-mail or Short Message Service (SMS or text messages) as long as these messages are not sent using a wireless Internet domain name on the FCC's published list.[256] Consequently, in the United States, the sending of truthful, nondeceptive unsolicited commercial electronic communications (e.g., e-mail) to consumers is generally lawful in the first instance, although consumers have the right to "opt-out" of receiving future communications by requesting that no more advertising be sent to them from a particular advertiser.[257] Also, telemarketing solicitations are generally lawful in the United States in first instance, so long as they are made by a real person (not solely through the use of autodialing equipment), although consumers may take action to prevent or stop such calls by listing their phone numbers on the National Do Not Call register or by making a company-specific do not call request.[258]

Overall, the United States lacks a broad data protection framework that would protect consumers in the context of RFID-enabled mobile phones used to deliver mobile advertising and location-based services and this creates an important regulatory gap. However, regulatory gaps exist in the European Union as well. First, applying the European Union's data protection framework to the context of RFID-enabled mobile phones used to deliver LBS and m-advertising is more challenging when there is no personal data used in the process because then E.U. data protection laws generally do not apply.[259] Furthermore, since generating advertising to RFID-enabled phones may be done without using the networks of public carriers, this also is a regulatory void that poses a risk to consumers' privacy.[260] Additionally, since tracking and profiling

---

lected and again on the occasion of each message in cases where the customer has not initially refused such use. *Id.* art. 13(2).

256. *See* King, *supra* note 27, at 254–65, 267–71.

257. For example, if an 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* U.S. Fed. Commc'n Comm'n, Consumer & Governmental Affairs Bureau, CAN-SPAM: Unwanted Text Messages and E-Mail on Wireless Phones and Other Devices (Nov. 5, 2008), http://www.fcc.gov/cgb/consumerfacts/canspam.html.

258. *See* discussion of the federal law restricting telemarketing practices, *supra* Part VI.B.1.

259. *See* discussion of the European Union's focus on regulating personal data protection, *supra* Part VI.A.

260. For example, it is possible for advertisers to send advertising to mobile phones without utilizing the services of a public carrier by including an ad in a message stored on RFID tags in smart posters. Consumers who use their phones to read the smart poster in order to obtain other desired information, like directions or product information, would also receive the advertising messages in direct communications between the smart posters and their phones

consumers using RFID-enabled mobile phones may be accomplished without using any personal data, this is a potential regulatory gap as well.[261]

In some respects, however, U.S. and E.U. laws are very similar. First, both laws require consumers to "opt-in" before it is lawful for advertisers to make autodialed telemarketing calls to mobile phones.[262] Since, as a practical matter, it is likely that marketers would use autodialing equipment to deliver m-ads by SMS/text messages because making live calls is likely to be more labor intensive and expensive, this type of m-advertising is only permitted with the mobile phone user's consent in both the United States and in the European Union.[263]

Second, using the Internet to generate electronic ads directly to mobile phones using wireless Internet domain names (as opposed to sending the ads to regular Internet e-mail addresses that mobile phone subscribers choose to access through mobile phones with Internet access) requires using wireless Internet domain names. So, in both the United States and the European Union, users' prior consents are required to send this type of m-advertising.[264] Third, in both the United States and the European Union, personal data gathered by mobile carriers that relates to the location of mobile phone users when they are making or receiving calls generally cannot be disclosed to third parties, such as businesses that provide location-based services (including mobile advertising), without obtaining the users' advance consent.[265]

Fourth, in both the European Union and the United States, consumers have legal protection that covers uses and disclosures of their personal data by m-advertisers and other businesses delivering LBS to the extent they have voluntarily adopted privacy policies—consumers can seek government enforcement if companies violate their own privacy

---

without the necessity of using telecommunications services. Spyware or adware is another possible way to generate m-advertising without using the services of a public carrier, although downloading software via the Internet to a mobile phone would utilize the services of public carriers like Internet Services providers. This is not the only way to load adware or software on mobile phones, however. For example, mobile phones could be sold with adware software pre-installed in order to facilitate m-advertising. *See* discussion and accompanying text, *supra* Part IV.

261. *See* discussion of profiling practices that do not use personal data, *supra* notes 140–142 and accompanying text.

262. *See supra* Part VI.A.1 (application of general rules) and Part VII.B.1–3 (application of specific rules), including discussion of federal laws in the United States that restrict telemarketing and the sending of commercial solicitations to mobile phone subscribers using wireless Internet domain names.

263. *See supra* Parts VI.A.1, VI.B.1 and accompanying text.

264. *See supra* Parts VI.A.1, VI.B.3.

265. *See supra* Parts VI.A.2, VI.B.3.

policies because this is an unfair trade practice.[266] Fifth, when consumer profiling practices do not use personal data, no legislation in either the United States or the European Union currently requires companies to make consumer profiles available to consumers (e.g., group classifications used for marketing purposes).[267] Additionally, as the laws in both the European Union and the United States are currently being interpreted, it is unlikely that tracking consumers in public places using anonymous but unique identifiers for marketing purposes is unlawful because both E.U. and U.S. laws only restrict disclosures by publicly regulated entities like mobile carriers, not marketers in general.

Next this article looks at new regulatory developments to see whether they are likely to being U.S. and E.U. law closer together in terms of regulating RFID applications for consumer devices, like the mobile phone.

VII. RFID Policy and Regulatory Developments in the European Union and the United States

Since 2006, the European Commission has been assessing the need to regulate the use of RFID technologies in Europe to protect individual privacy and personal data.[268] It has sponsored several workshops on RFID themes for participants from academia, industry and regulatory bodies and has obtained comments from the public through an online forum.[269] Although the European Commission's regulatory efforts focus

266. *See* discussion of unfair commercial practices acts in the European Union and the United States, *supra* notes 178–179 and accompanying text.

267. *But see* discussion of the Data Protection Directive and the possibility that Article 15 may apply to automated decisions that do not use personal data, *supra* note 140 and accompanying text. *See also infra* Part VI.B.2 (discussing the FTC's proposed guidelines on online behavioral advertising).

268. *See* European Commission, Directorate General Information Society & Media, *Towards an RFID Policy for Europe: Workshop Report*, DRR-4046-EC (Aug. 31, 2006) (*prepared by* Maarten Van De Voort & Andreas Ligtvoet); *see also* Speech, Viviane Reding, Member of the European Commission responsible for Information Society and Media, The RFID Revolution: Challenges and Options for Action, International CeBIT Summit, Hannover (Mar. 9, 2006), http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/06/162&format=HTML&aged=1&language=EN&guiLanguage=en [hereinafter Reding Speech]; Jonathan Collins, *European Commission Works on RFID Policy*, RFID J., Mar 14, 2006, http://www.rfidjournal.com/article/articleprint/2197/-1/1/.

269. *See, e.g.*, EDPS Opinion on RFID, *supra* note 20. The European Commission is required to consult with the EDPS when a proposal for legislation has a possible effect on data protection. *See* Opinions, EDPS, http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/82 (last visited Jan. 4, 2009) ("The EDPS analyses the proposal, taking into account the main elements affecting data protection . . . . The EDPS makes constructive recommendations to improve the proposal in this respect. The opinion of the EDPS is formally issued and then forms part of the legislative process.").

on RFID use in Europe, spokespersons have also stated that the European Commission is "stepping up efforts to join with the United States and Asian countries in defining globally accepted RFID interoperability standards, data-privacy practices and ethical principles" for applying the technologies.[270] Likewise, the U.S. government, and particularly the FTC, has been considering the need to regulate the use of RFID technologies in the United States. The FTC has also held RFID workshops on RFID themes.[271]

European Union-level policy-makers have closely examined new business practices that implement RFID technologies to determine if they create significant privacy and data protection concerns (as well as security concerns) for E.U. citizens. The analysis produced in this effort is insightful, comprehensive and well-documented, providing a rich foundation for discussions about privacy and data protection on the topic of this paper. In contrast, this type of regulatory focus in the United States is primarily taking place at the state level with the introduction of state legislation on RFID to protect consumers' privacy and security. But there are also important developments in the United States that focus on regulating the online marketing practices to protect consumers. For example the FTC has published guidelines on online behavioral marketing practices that collect personal data, profile and track consumers. These guidelines address some of the same privacy concerns identified earlier in this paper that arise from using RFID-enabled mobile phones and RFID-embedded consumer environments to deliver LBS and mobile advertising.

A. *Regulatory Developments in the European Union*

The European Commission has the power to initiate legislation to regulate the use of RFID and address the privacy and data protection issues related to RFID.[272] In 2007, the European Commission announced that the time had not yet come to adopt RFID regulations for Europe in view of the continuing development of RFID technology and evolving business applications of RFID.[273] Rather than adopting new laws, the

270. EC Communication on RFID, *supra* note 197, at 5; Collins, *supra* note 268.

271. *See, e.g.*, *FTC Workshop Report*, *supra* note 50, at 2.

272. EC Communication on RFID, *supra* note 197, at 10–11 (discussing the interplay of European and Member-States' laws in the regulation of data protection in the European Union and the timeframe for European Commission policy-making and consideration of the need for new legislation to address RFID usage in the European Union).

273. *Id.* (reporting that by the end of 2007, the Commission will issue a recommendation setting out the principles that public authorities and other stakeholders should apply to RFID usage, will consider including appropriate provisions in the forthcoming proposal to amend the E-Privacy Directive 2002/58/EC, (*see supra* note 185), and will take into account input from the forthcoming RFID Stakeholder group and the Article 29 Data Protection Working

European Commission announced that it planned to develop a set of guidelines (so-called "soft law") that would lay out its expectations on issues such as privacy and security with respect to the use of RFID technologies.[274] To date, no new legislation has been proposed or adopted by the European Commission to specifically regulate the use of RFID technologies in Europe. However, as discussed in the second part of this section, the European Commission has issued draft recommendations addressing the privacy, data protection and information security principles for applications supported by RFID technologies. The proposed recommendations, together with other recent policy-making and regulatory actions of the European Commission, significantly advance the discussion of the privacy and data protection implications of RFID technologies and whether new government regulation or industry self-regulation, or some combination of the two approaches, is needed to protect consumers' privacy.[275] While some of the European Union developments focus on broad data protection regulation rather than RFID, they are discussed here because they include analysis of the use of RFID technologies in Europe. What follows is a chronological discussion of the policy-making and regulatory efforts of the European Commission, beginning in 2007.

1. Recent Policy Focus on RFID

In early 2007, the European Commission issued its Communication on RFID.[276] In this Communication, the European Commission characterized RFID information systems and associated security and privacy risks as a "moving target" that will "require continuous monitoring, assessment, guidance, regulation, and [research and development]."[277] The European Commission stated, "The specific security and privacy risks largely depend on the nature of the RFID applications," so a one-size-fits-all approach would not be appropriate.[278] Furthermore, the European Commission stated that "[p]rivacy and security should be built into the

---

Party. By the close of 2008, the Commission plans to reevaluate whether legislation is necessary.). However, if fundamental privacy rights are not protected by future uses of the technology, regulations will likely follow. Anne Broache, *E.U. Official: Now Isn't Time for RFID Regulations*, ZDNET AUSTRALIA, Apr. 3, 2007, http://www.zdnet.com.au/news/security/soa/EU-official-Now-isn-t-time-for-RFID-regulations/0,130061744,339274657,00.htm.

274. Broache, *supra* note 273. *See also* EC Communication on RFID, *supra* note 197, at 10–11.

275. *See* discussion of European Union regulatory reforms, *infra* Part VII.A.2.

276. E.C. Communication on RFID, *supra* note 197. In this Communication, the European Commission announced that an RFID Stakeholder Group would be established for two years and include representatives of consumer groups, market actors (industry) and national and European Union government authorities, including data protection authorities. *Id.* at 9.

277. *Id.* at 6.

278. *Id.*

RFID information systems before their widespread deployment ('security and privacy-by-design'), rather than having to deal with it afterwards."[279] The European Commission also noted that since "end users typically are not involved in the technology design stage, the Commission will support the development of a set of application-specific guidelines (code of conduct, good practices) by a core group of experts representing all parties."[280]

In addition to its Communication on RFID, the European Commission issued a communication to the European Parliament and the Council on the follow-up of the Work Program for better implementation of the Data Protection Directive (2007 E.U. Communication on Data Protection).[281] This Communication on Data Protection stated the European Commission's conclusion that the Data Protection Directive continues to be relevant in its role in providing a general framework for data protection and fulfilling its objectives to guarantee a high level of data protection; thus, it does not need to be amended.[282] The European Commission stated its intention to take up the challenges of new internet and communications technologies and said it may propose specific legislation at the European Union level in order to apply those principles to specific requirements of the technologies, analogous to the approach in the E-Privacy Directive.[283]

In June 2007, the Commission issued a decision to formally create the Expert Group on Radio Frequency Identification, as had been previously announced in its Communication on RFID.[284] This group was established to provide advice to the European Commission on RFID usage and is responsible for developing "guidelines on how RFID applications should operate taking into account the views of stakeholders and issues relating to long-term users as well as economic and societal aspects of RFID technologies."[285] Also in June 2007, the Article 29 Data

279. *Id.* at 9.

280. *Id.*

281. *See generally* EC Communication on Data Protection, *supra* note 164.

282. *Id.* at 9 (stating that the Data Protection Directive "gives shape to the fundamental right to protection of personal data . . . [and] [t]herefore the Commission does not envisage submitting any legislative proposal to amend the Directive", but "will produce an interpretive communication on some provisions.").

283. *Id.* at 10. One accomplishment listed was the Working Party's approval of the European Code of Conduct of the Federation of European Direct Marketing (FEDMA), which it characterized as an important milestone, despite lack of progress in similar industry self-regulatory efforts. *Id.* at 5.

284. Commission Decision 467/2007, art. 1, 2007 O.J. (L 176), 25 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/l_176/l_17620070706en00250030.pdf [hereinafter Decision 467/2007/EC]. *See also* EC Communication on RFID, *supra* note 197, at 9–10.

285. Decision 467/2007, *supra* note 284, art. 2(b).

Protection Working Party again joined the discussion when it issued an Opinion on the concept of personal data.[286] The Opinion discussed the applicability of the definition of personal data to the RFID context and identified telephone location data and call log data as personal data, two concepts that are very important for discussions of mobile advertising.[287] The Opinion also analyzed whether Internet Protocol (IP) addresses are data relating to identifiable persons and therefore covered by the Data Protection Directive. It found IP addresses are personal data in the context of processing them to identify the users of computers (for example, to identify copyright infringers), but also acknowledged that certain types of IP addresses that do not allow identification of the user may not be personal data (for example, IP addresses attributed to a computer in an internet café, where no identification of the user is requested).[288] Going further, relating to discussions about whether recording unique identifiers on RFID tags may generate personal data, the Opinion stated that for the processing of data to be covered by the Data Protection Directive, it may not be necessary in all cases to be able to identify individuals by name.[289]

---

286. Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data*, 01248/07/EN, WP 136 (June 20, 2007), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf [hereinafter Opinion 4/2007]. In this opinion, the Working Party analyzed in depth the concept of "personal data" that should be covered by the Data Protection Directive, breaking the definition into four distinct elements: (1) "any information," (2) "relating to," (3) "identified or identifiable," [natural persons] and (4) "natural persons." *Id.* at 3–24.

287. *Id.* at 3, 10, 26. "In the context of discussions on the data protection issues raised by RFID tags, the Working Party noted that 'data relates to an individual if it refers to the identity, characteristics or behavior of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated.' " *Id.* at 10. The Opinion stated the intention of the Working Party to contribute to further analysis of the way in which data protection rules may impact the use of RFIDs and the possible need for additional measures that may be necessary to protect data protection rights. *Id.* at 26. The Opinion also discussed situations where location data (here, generated by a system of satellite location set up by a taxi company, i.e. GPS) makes it possible to determine the position of available taxis in real time. *Id.* at 11. The Working Party concluded that the location data can be considered to be personal information about taxi drivers and was subject to the data protection rules, even though the purpose of the processing was to provide better customer service and to save fuel, not to monitor the performance of taxi drivers, because the system allowed for monitoring taxi drivers' performance. *Id.* Likewise, call log information for a telephone located inside a company office could be personal data of employees using the phone and the cleaning staff who might also use the phone. *Id.* The concept of personal data extended to both outgoing and incoming calls insofar as all of them contain information about people's private life, social relationships and communications. *Id.*

288. *Id.* at 16–17.

289. For example:

> Computerized files registering personal data usually assign a unique identifier to the persons registered, in order to avoid confusion between any two persons in the file . . . and web traffic surveillance tools make it easy to identify the behaviour of a

In July 2007, the European Data Protection Supervisor (EDPS) provided his opinion on the European Commission's Communication on Data Protection.[290] The EDPS agreed with the European Commission's Communication that, in the short-run, the Data Protection Directive should not be amended and that review of the E-Privacy Directive needs to be conducted to assess the possible need for more specific rules to address data protection issues raised by new technologies such as the Internet and RFID.[291] However, the EDPS expressed serious reservations about other points in the European Commission's Communication and questioned whether it was unavoidable that the Data Protection Directive would need to be amended in the longer term.[292] The EDPS Opinion also suggested that the European Commission set a timeline for its activities, such as the preparation of a report on the implementation of the Data Protection Directive,[293] argued that there needs to be a long-term approach to resolve data protection issues in the context of a developing surveillance society,[294] and regretted that the European Commission did not more adequately address the perspective of global privacy and jurisdiction and practical solutions to provide global solutions.[295]

> machine and, behind the machine, that of its user. Thus the individual's personality is pieced together in order to attribute certain decisions to him or her . . . [and] the definition of personal data reflects this fact.

Id. at 14, ex.10.

290. EDPS Opinion on Data Protection, *supra* note 186.

291. *Id.* at 11, ¶¶ 75–76 (summarizing conclusions more fully developed earlier in the document).

292. *Id.* at 11, ¶ 77 (summarizing conclusions more fully developed earlier in the document).

293. *Id.* at 11, ¶ 78 (summarizing conclusions more fully developed earlier in the document).

294. *Id.* at 11, ¶ 79 (summarizing conclusions more fully developed earlier in the document).

295. *Id.* at 11, ¶ 80 (summarizing conclusions more fully developed earlier in the document). In this regard, the EDPS recommended that the EC consider:

> [F]urther development of a Global Framework for data protection; the further development of the special regime for transfer of data to third countries; international agreements on jurisdiction or similar agreements with third countries; investing in mechanisms for global compliance, such as the use of binding corporate rules by multinational companies.

Id. The EDPS invited the EC to start developing a vision on this perspective that would involve major stakeholders. *Id.* 6–77, ¶¶ 38–45 (discussing more specifically the recommendations of the EDPS to the EC to address the global privacy and jurisdiction issues related to implementing the Data Protection Directive, including citations to work that had previously been done).

Also in July 2007, the European Commission issued its final version of "European Union, European Policy Outlook RFID."[296] In this policy statement, the European Commission discusses the policy challenges relative to RFID technologies, while stopping short of recommending RFID-specific legislation to protect privacy.[297] It identified the need for fair rules for privacy and governance of RFID as both a major opportunity and challenge, noting that the potential invisibility of radio frequency identification "demands a comprehensible and reliable approach to preservation of data protection, workers' rights and consumer rights in those RFID applications that may be used to track people or to build personal data profiles."[298] It also encourages the acceleration of broad public usage and RFID acceptance in areas providing added value to the end user, for example, the development of "mobile phones with RFID reader functionalities as the human interface to wireless sensor networks."[299]

Subsequently, in November 2007, the European Commission issued a proposal to amend two existing directives, including the E-Privacy Directive.[300] One of the proposed amendments to the E-Privacy Directive

---

296. Berlin Conference, *European Policy Outlook RFID: Final Version*, at 7 (July 2007) (defining "ubiquitous computing" and "The Internet of Things"), *available at* http://www.nextgenerationmedia.de/documents/European_Policy_Outlook_final_version.pdf [hereinafter RFID Policy Statement].

297. *Id.* at 30 (commenting that "[c]urrently, a special RFID law seems counterproductive, since data protection legislation should remain as it is now: technology-neutral" and that "[s]elf-regulation should be used to supplement regulatory measures, particularly in areas that are too specific to be addressed by legislation.").

298. *Id.* at 35. The notion that data protection regulation should include informed consent provoked discussion of the technical challenges to this concept posed by RFID:

> The issue of ubiquitous data processing and storage raises a challenge in terms of informed consent . . . to the processing of individual-related data to be maintained in an environment of hundreds of smart objects communicating (partially) autonomously. New technical and organizational concepts are likely to be needed to maintain informed consent. Resolving the challenge of informed consent in a ubiquitous environment must consider the features, possibilities and functional logic of smart objects on the one hand, and the permanent awareness of "yes/no" decisions and its practicability on the other hand.

Id. at 39–40.

299. *Id.* at 37–38. The RFID Policy Statement makes recommendations for data protection and consumer awareness to include the need to review data protection law at regular intervals and to amend regulations as needed so that the law is adequate to address "the rapidly increasing interconnectedness of IT systems, mobile devices and everyday objects." *Id.* at 41–42. It also discusses the use of self-regulation, such as commitment by RFID users to a universal and enforceable code of conduct, to supplement regulatory measures. *Id.* at 42.

300. *Proposal for a Directive of the European Parliament and the Council Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No*

clarifies that the directive also applies to "public communications networks supporting data collection and identification devices including contactless communications devices such as Radio Frequency Identification devices".[301] The European Commission explains:

> Radio Frequency Identification Devices (RFID) use radio frequencies to capture data from uniquely identified tags, which can then be transferred over existing communications networks. The wide use of such technologies can bring considerable economic and social benefits and thus make a powerful contribution to the internal market if their use is acceptable to citizens. To achieve that, it is necessary to ensure that the fundamental rights of individuals, in particular the right to privacy and data protection, are safeguarded. When such devices are connected to publicly available electronic communications networks or make use of electronic communications services as a basic infrastructure, the relevant provisions of Directive 2002/58/EC, including those on security, traffic and location data and on confidentiality, should apply.[302]

The proposed amendments to the E-Privacy Directive requires Member-States to protect consumers from unauthorized access and storage on their terminal equipment and is not limited to intrusions accomplished using publicly available electronics communications networks:

> [T]he storing of information, or gaining access to information already stored, in the terminal equipment of a subscriber or user is

---

2006/2004 on Consumer Protection Cooperation, COM (2007) 298 final (Nov. 13, 2007), *available at* http://ec.europa.eu/information_society/policy/ecomm/doc/library/proposals/698/com_2007_0698_en.pdf (clarifying that the Directive also applies to public communications networks supporting data collection and identification devices (including contactless devices such as Radio Frequency Identification devices)); *see generally* E-Privacy Directive, *supra* note 185.

301. The European Commission is proposing to amend Article 3 of the E-Privacy Directive to define "services concerned" as follows: "This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Community, including public communications networks supporting data collection and identification devices." *Id.* at 33. *See also id.* at 6, 12. The proposed amendments to the E-Privacy Directive also define "call" to mean "a connection established by means of a publicly available telephone service allowing two-way communication." *Id.* at 32. Other proposed changes to the E-Privacy Directive include user notification requirements for security breaches relating to users' personal data; allowing Internet Service Providers to take legal action against spammers; and clarifying that use of "spyware" remains illegal in the European Union regardless of the means of deployment. *Id.* at 11–12.

302. *Id.* at 19.

> only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with [the Data Protection Directive] . . . about the purposes of the processing and is offered the right to refuse such processing by the data controller.[303]

In the m-commerce and m-advertising context, for example, this amendment will clarify that consumers with mobile phones will be entitled to notice before their public mobile phone service providers, public Internet service providers *or anyone else* may store information on their mobile phones or access data already stored on their mobile phones because mobile phones are terminal equipment of the subscriber used in a public electronics communication network. Thus, mobile advertisers and other businesses that use RFID readers to access personal information stored on consumer's mobile phones would be required to give notice of the purposes of the processing and an opportunity to decline the access and processing of their personal data.[304] Also, if a mobile advertiser uses the Internet to convey personal data of a mobile subscriber that has been collected using RFID technologies, the amended E-Privacy Directive would apply. For personal data that is collected or otherwise processed by RFID systems without using a public carrier's network or access or storage on the consumer's terminal equipment, the general Data Protection Directive would continue to apply.

In December 2007, the European Data Protection Supervisor issued an opinion on the European Commission's Communication on RFID. The EDPS Opinion on RFID also responds to other significant actions on RFID by the European Commission and by the Article 29 Data Protection Working Party that occurred in 2007, including the European Commission's proposal to amend the E-Privacy Directive.[305] The EDPS

---

303. *Id.* at 33–34. This amendment would replace Article 5(3) of the E-Privacy Directive that only applied to the use of electronic communications networks (public carriers) to store information or access information on the user's terminal equipment. E-Privacy Directive, *supra* note 185, art. 5(3).

304. *Id.* Exceptions to the requirement to obtain notice and consent before accessing or processing subscribers' or users' data on the terminal equipment of the subscriber or user include: (1) technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or (2) as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user. *Id.* at 34, ¶ 4.

305. *See* EDPS Opinion on RFID, *supra* note 20, at 2; *see also* Press Release, EDPS Opinion on RFID: Major Opportunities for Information Society But Privacy Issues Need To Be Addressed With More Ambition, EDPS/07/13 (Dec. 20, 2007), *available at* http://www.europa.eu/rapid/pressReleasesAction.do?reference=EDPS/07/13&format=HTML&aged=0&language=EN&guiLanguage=en. The European Commission is required to consult with the EDPS when a proposal for legislation has a possible impact on data protection. *See* Consultation, EDPS, http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/80 (last visited

Opinion on RFID states that RFID qualifies as a fundamentally new technological development which raises important questions about data protection and privacy.[306] First, examining the practical consequences of the deployment of RFID-systems for data protection and privacy, the EDPS states that in assessing the data protection and privacy concerns associated with this fundamental new technology, it is important to consider the consequences of the overall RFID infrastructure that includes "the tag, the reader, the network, the reference database and the database where the data produced by the association tag/reader is stored," as opposed to only focusing on RFID tags.[307] Next, the EDPS Opinion on RFID analyzes the impact of RFID on privacy and data protection, first providing a description of how these fundamental rights are protected under the present legal framework, and then analyzing the possibilities of fully using the present legal framework to protect privacy and data

---

Jan. 2, 2009). *See also Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council Amending, Among Others, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*, 2008/C 181/01, OJ (C 181/1) (Apr. 10, 2008), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:181:0001:0013:EN:PDF [hereinafter EDPS Opinion on Proposed E-Privacy Amendments].

306. EDPS Opinion on RFID, *supra* note 20, at 3 (limiting the EDPS Opinion to questions of data protection and privacy but recognizing that important questions are also raised in other areas).

307. *Id.* at 3. The EDPS outlines key privacy and data protection issues that need to be addressed concerning RFID tags and concerning RFID system deployment, listing five basic issues at the system deployment level: (1) Identification of the data subject by RFID systems and the need to do so in a data protection friendly way; (2) Identification of the controller who is responsible for processing personal data according to the data protection legal framework, recognizing the during the lifecycle of an RFID tag, the controller who processes the data may change several times as additional services are provided in relation to the tagged object; (3) Decreased meaning of the traditional distinction between the personal and public sphere in the context of RFID technologies that may not be apparent to the data subject, including the wireless nature of the tag communication, its ability to be read outside line-of-sight and its evolving reading range; (4) The consequences of the size and physical properties of RFID tags (recognizing that the goal of making tags small and cheap for purposes of commercial feasibility also minimizes the likelihood of the tag including security measures and that wireless communication is a feature of the tags which adds a layer of risk and supports a need for additional security features); (5) the lack of transparency of the processing of personal data that is enabled by RFID systems, which may lead to unnoticed gathering and processing of information capable of being used to profile individuals. The opinion compares RFID systems to mobile phones, in terms of the likelihood that RFID technology, like mobile phone technology, will be widely accepted by users despite its potentially intrusive privacy risks. The opinion says the two technologies are distinguishable, however, in that mobile phones are visible and can be turned off by users, while RFID chips and systems are not under the control of the user and cannot be turned off. *Id.* at 5–6. The EDPS Opinion does not consider the possibility of converging technologies such as the context discussed in this paper in which mobile phones may contain RFID tags and readers. When mobile phones are RFID-equipped and consumer environments embedded with RFID tags and readers, even if this is not a universal situation, heightened user tracking and lack of transparency of processing may also potentially impact user acceptance of such mobile phone technologies.

protection.[308] The EDPS makes the point that the interaction between new technological developments like RFID and the requirements for an effective legal framework for data protection are complex because "the technology influences the legislation and the legislation influences the technology."[309] Specifically, the EDPS recommends that the opt-in principal be made the cornerstone of RFID regulation from a data protection standpoint, whether by legislation or self-regulation.[310]

The EDPS opinion advises that, in most situations, the "opt-in-principle" at the point of sale is a legal obligation that already exists under the Data Protection Directive, although there is good reason to specify this obligation in self-regulatory instruments to ensure that it will be implemented in the most appropriate way. It should also specify that this principle applies to RFID applications that fall outside the scope of the Data Protection Directive.[311] Further, the EDPS welcomes the

---

308. *Id.* at 6.

309. *Id.*

310. *Id.* at 9. The opinion lists potential non-binding self-regulatory (non-legislative) instruments relevant to RFID regulation, including: interpretative communications or other communications, promotion of best practices, the use of privacy seals and third-party privacy audits, including the codes of conduct or good practice that the European Commission, "in consultation with the RFID-Stakeholders Group, is expected to stimulate and to steer this process of self-regulation" utilizing guidelines that public authorities and other stakeholders should apply for RFID usage. *Id.* at 7–8.

311. *Id.* at 10, 17. For RFID applications that fall outside of the scope of the Data Protection Directive, the EDPS advises that specific implementation is needed (without specifying what those applications may be). *Id.* Later in the opinion, while arguing for adoption of a tailor-made legal framework to consist of a mix of regulatory tools which specify and complement the existing legal framework, the EDPS argues that tailor-made legislation might be needed, because:

> [N]ot all RFID applications entail the processing of personal data. In other words, if RFID applications do not entail the processing of personal data, parties involved in the manufacturing and selling of RFID enabled products are not legally bound to implement any technological measures that would prevent eavesdropping or the setting up of readers without proper notice to individuals. Yet, as demonstrated, privacy risks derived from the possible surveillance of individuals also exist for such RFID applications, thus demanding the same type of privacy safeguards. Precisely, this may be the case for item level tagging in consumer products *before* the point of sale. In sum, RFID applications that do not process personal data may still threaten individuals' privacy by enabling surreptitious surveillance and the use of the information for unacceptable purposes.

Id. at 14. *See also supra* Part V (discussing the privacy implications of profiling based on RFID and other technologies that produce ambient intelligence based on autonomic computing capabilities and why use of these technologies by advertisers to generate customer profiles may fall outside data protection regulation). RFID and other technologies that produce ambient intelligence, and the automatic customer profiling enabled through their use produce knowledge about groups of customers from aggregated customer data, have consequences for individual customers, although they may be unaware of the implications of the profiling; thus "raising . . . questions in relation to privacy and security; especially with regard to data protection legislation." Hildebrandt, *supra* note 65, at 6–7, 16–17 (arguing for effective transparency

European Commission's endorsement of specification and adoption of early design criteria to minimize privacy and data protection threats (so called "privacy by design," including Best Available Techniques or "BATs"). However, the EDPS opinion questions the effectiveness of soft law approaches for regulation of RFID uses in Europe and advocates adoption of legislation to regulate the main issues of RFID usage in case the effective implementation of the existing legal framework fails.[312] Finally, the EDPS calls for more efforts to address the "inherently trans-border" dimension of RFID systems at an international level. The EDPS noted that RFID systems are already trans-border, as the activity of an RFID tag might not stop at the point of sale.[313] Also, from the level of overall RFID systems, it is necessary to consider the privacy implications of transfers of personal data about E.U. citizens made to a third country by a producer of the tagged item that is based outside the European Union.[314]

2. European Union Releases Draft RFID Recommendations

In February 2008, the European Commission issued a Draft RFID Recommendation addressing the privacy, data protection and information security principles for applications supported by RFID and solicited comments on its recommendation.[315] The comment period has

---

enhancing tools (TETs) that create profiles which are both both accessible and assessable and that may affect the lives of people, as opposed to privacy-enhancing technologies that focus on hiding of data or anonymization).

312. *See* EDPS Opinion on RFID, *supra* note 20, at 13. Referencing the European Commission's Communication on RFID, the EDPS comments:

> The [EC] refers to RFID as the gateway to a new phase of development of the Information Society, often referred to as the "internet of things" and RFID tags will constitute key elements of the "ambient intelligent" environments. These environments are also important steps in the development of what is often called the "Surveillance Society".

Id. Thus, the EDPS concluded, "Against this background, legislative action in the area of RFID can be justified. RFID may bring about a qualitative change." *Id.*

313. *Id.* at 15.

314. *Id.* The EDPS also noted the need to address governance of RFID identity reference databases as a critical dimension for appropriate enforcement of the E.U. data protection legal framework. *Id.*

315. European Commission, *Introduction to the Public Consultation on the RFID Privacy, Data Protection and Security* (2008) [hereinafter *Draft RFID Recommendation*] (the period to comment ended April 25, 2008). As of the date of this writing, the European Commission had not issued final RFID recommendations. *See also* ANEC & BEUC, *Radio Frequency Identification (RFID) Draft Commission Recommendation on the Implementation of Privacy and Information Security Principles in Applications Supported by Radio-Frequency Identification—"RFID Privacy and Security Recommendation"*, http://www.anec.org/attachments/ANEC-ICT-2008-G-017final.pdf (presenting, in full, the text of the European Union's Draft RFID Recommendations and the joint comments thereto by the ANEC and

closed and the European Commission is expected to issue final RFID guidance soon.[316] The Draft RFID Recommendation provides "guidance" to Member-States and stakeholders on the design and operation of RFID applications in a "lawful, ethically admissible and socially and politically acceptable way, respecting the right to privacy and ensuring protection of personal data and appropriate information security."[317] The Draft RFID Recommendation is not binding law, although it does not preclude Member-States from adopting binding legislation.[318]

Article 7 of the Draft RFID Recommendation covers RFID use in retail applications and provides advice on providing notice and obtaining consumers' consent, specifying when "opt-in", as opposed to "opt-out", consent should be given by consumers.[319] Article 7 recommends harmonized signs to notify consumers of the presence of an RFID tag in a retail product and discusses the content of notices to consumers. It suggests a notice to inform consumers: (1) of the presence of a RFID tag in a retail product; (2) whether the tag has a specified, explicit and legitimate purpose after sale; (3) about the likely reasonable privacy risks relating to the presence of the tag; and (4) of measures consumers can take to mitigate these risks.[320]

When the operation of the specific RFID application associated with the tag involves processing personal data, Article 7 states that a retailer must comply with the Data Privacy Directive in terms of legitimately processing personal data, and needs to either deactivate the RFID tag at the point of sale or obtain consumer consent to receive a product with an active RFID tag ("opt-in" consent).[321] Retailers are advised to conduct

---

BEUC). *See also* BEUC, the European Consumers' Organisation, http://www.beuc.eu (last visited Jan. 16, 2009); ANEC, The European Consumer Voice in Standardisation, http://www.anec.eu (last visited Jan. 16, 2009).

316. *See EC Opens Comment on RFID Recommendations*, ELECTRONIC PRIVACY INFORMATION CENTER, Feb. 25, 2008, http://epic.org/privacy/rfid/.

317. *Draft RFID Recommendation*, *supra* note 315, art.1. Article 10 of the Draft RFID Recommendation specifies that the European Commission will provide a report on the implementation of this Recommendation and its impact on economic operators and consumers within three years. *Id.* art. 10. Additionally, the European Commission stated that, "[W]here appropriate, [it] may amend this Recommendation or submit any other proposal it may deem necessary, including binding measures, in order to better achieve the goals of the Recommendation." *Id. See also Data Protection Directive*, *supra* note 97; E-Privacy Directive, *supra* note 185.

318. *See Draft RFID Recommendation*, *supra* note 315, art. 1.

319. *Id.* art. 7.3. In its commentary preceding draft Article 7.3, the European Commission explains: "In accordance with Directive 95/46, the article recommends that tags that contain personal data should be subject to the 'opt-in' principle at the point-of-sale, that is tags are [to be] deactivated by default unless the consumer wants to keep them active." *Id.* (explanatory comments to Article 7).

320. *Id.* art. 7.2.

321. *Id.* art. 7.3.

privacy impact assessments to determine if an RFID application associated with a tag that will be active after sale involves processing personal data. If the privacy impact assessment conducted by the retailer shows a significant likelihood of personal data being generated from the use of the RFID application, then the retailer should either deactivate the tag or obtain consumer consent to receive an RFID-tagged retail product that will be active post-sale.[322] On the other hand, where an RFID application does not involve processing of personal data (or where the privacy impact assessment has shown negligible risk of personal data being generated through the application), the Data Privacy Directive is not applicable and the retailer need not obtain consumer consent to sell a retail product with an active RFID-tag. Where personal data will not be processed post-sale by an RFID application, the retailer should still provide an easily accessible facility to deactivate or remove the tag. Thus, the Draft RFID Recommendation essentially establishes an "opt-out" consent procedure for applications that do not process personal data in which the tag may remain active unless the consumer takes action to request deactivation of the tag.[323]

When deactivation of an RFID tag in a consumer product is required at the time of sale (for example, if the tag contains personal data) or if deactivation is requested by the consumer, the guidelines state that deactivation or removal of RFID tags should not reduce or terminate any of the legal obligations of the retailer or manufacturer toward the consumer (e.g., warranty service rights).[324] Furthermore, deactivation or removal of the tags by the retailer should be done immediately and free of charge to the consumer.[325] Finally, consumers should be able to verify that the action to deactivate the tag is effective.[326]

Despite the advisory nature of the European Commission's Draft RFID recommendations, supporters of the RFID industry argue that if they are not revised, they potentially will undercut the value of RFID to deliver value to companies and consumers across Europe. These industry supporters argue the recommendations lack balance between protecting the public and overregulation that will stifle technical adoption and innovation.[327]

---

322. *See infra* Part IX.A.

323. *Draft RFID Recommendation*, *supra* note 315, art. 7.3. *See also* Information Commissioner's Office, United Kingdom, Privacy Impact Assessment Handbook, http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html (last visited Jan. 2, 2009) [hereinafter ICO PIA Handbook].

324. *Draft RFID Recommendation*, *supra* note 315, art. 7.4.

325. *Id.*

326. *Id.*

327. *See* Mark Roberti, *Give Your Views to the EU—Now!*, RFID J., Apr. 7, 2008, at 2, http://www.rfidjournal.com/article/articleview/4003/1/128/.

B. *Regulatory Developments in the United States*

Compared to the regulatory focus on the privacy implications of commercializing RFID technologies that has taken place in the European Union, there has been almost no regulatory focus on RFID or m-advertising practices in the United States, at least at the federal level. Early on, the FTC,[328] the leading federal agency charged with protecting consumers from unfair and deceptive business practices, held workshops to assess the potential effect of RFID technologies on consumers. Subsequently, the FTC chose to encourage self-regulatory efforts by the RFID industry as opposed to supporting the adoption of new laws to address applications of RFID.[329] In 2008, the FTC held two workshops to investigate the security and privacy implications of contactless payment systems that utilize radio frequency identification and the various devices used for contactless payment systems, indicating that it may be taking a closer look at new applications of RFID, including the security and privacy issues associated with RFID-enabled consumer devices.[330] To date, however, most of the developments in the United States related to regulating RFID are taking place at the state level, including the introduction of RFID-specific state legislation, as described in the next section. On the other hand, there have been recent federal-level developments that focus on protecting consumers' privacy and personal data related to online marketing practices, in the form of FTC proposed guidelines for behavioral marketing practices. These proposed guidelines address many of the same privacy and data protection issues identified with respect to delivering LBS and m-advertising using RFID-enabled

---

328. 15 U.S.C. § 57a(a)(1)(b) (2008) (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 at http://www.ftc.gov (last visited Jan. 16, 2009).

329. *See FTC Workshop Report*, *supra* note 50, at 21–23; *see also* Jonathan Collins, *FTC Asks RFID Users to Self-Regulate*, RFID J., Mar. 10, 2005, http://www.rfidjournal.com/article/view/1437/1/1/. Of course, in the future, the FTC could change its position favoring industry self-regulation with respect to RFID applications and use its existing enforcement powers to more closely scrutinize new applications of RFID technologies that effect consumer privacy and data protection.

330. *FTC to Host Another Workshop on RFID Privacy Concerns, Contactless Payments*, CONTACTLESSNEWS, Aug. 21, 2008, http://www.contactlessnews.com/2008/08/21/ftc-to-host-another-workshop-on-rfid-privacy-concerns-contactless-payments. *See also FTC to Scrutinize Contactless Payment Technology*, NETWORKWORLD, May 12, 2008, http://www.networkworld.com/community/node/27710 (noting that contactless payment technology uses RIFD chips embedded in smart cards, mobile phones, or USB devices to enable consumers to make debit and credit transactions, typically for low value purchases by holding an RFID-enabled device in proximity to an RFID reader). The BART-RFID Trial is an example of consumers using contactless payment technology enabled through their RFID-enabled mobile phones in an RFID-embedded environment. *See supra* Part III for a discussion of this consumer trial.

mobile phones such as privacy concerns associated with consumer tracking and profiling for marketing purposes. Congress has also begun investigating whether there is a need to regulate online behavioral marketing practices to protect consumers' privacy and security.[331]

1. State RFID Legislation

At the state level, there have been some regulatory efforts to address the commercialization of RFID technologies through legislation designed to protect consumers' privacy. In 2008, Washington enacted the first RFID-specific state legislation of its type, making it a criminal offense to "skim" an RFID device, defined to cover the intentional scanning of another person's identification device without that person's prior knowledge and consent for the purpose of fraud, identity theft or any other illegal purpose.[332] Proposed language in the bill would have made it a felony for any company or person to slip an RFID chip into a cell phone, loyalty card, or other device without that person's prior knowledge and consent.[333] However, this provision was omitted from the final bill that was adopted into law. Also omitted from the new law was a provision that would have made it unlawful to read an RFID tag containing a consumer's personal information without her notice and consent and to use that information for marketing purposes.[334]

California also passed an anti-skimming bill that makes it a crime to intentionally remotely read someone's RFID data on an identification

---

331. Congress held hearings in 2008 to investigate whether there is a need to regulate online behavioral advertising practices to protect consumers' security and privacy. Joelie Tessler, *Microsoft, Google Back Broad Privacy Legislation*, SFGATE.COM, July 9, 2008, http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2008/07/09/financial/f125127D29.DTL (reporting on a Senate Commerce Committee hearing on online advertising).

332. Electronic Communication Devices, REV. CODE WASH. § 19.300.020 (2008) (effective June 12, 2008, adding a new chapter to Title 19 RCW, and making it a felony to "intentionally [scan] another person's identification device remotely, without that person's prior knowledge and consent, for the purpose of fraud, identity theft, or for any other illegal purpose"). *See also* Kristi Heim, *State Leads Way on RFID Privacy*, SEATTLE TIMES, Mar. 31, 2008, at C4; Claire Swedberg, *Washington State Governor Signs Anti-Skimming Law*, RFID J., Mar. 27, 2008, http://www.rfidjournal.com/article/articleprint/3988/-1/1/.

333. *See* Heim, *supra* note 332, at C4.

334. *See* Claire Swedburg, *Washington State House Gives Nod to Privacy Bill*, RFID J., Feb. 15, 2008, http://www.rfidjournal.com/article/articleprint/3928/-1/1. The 2008 Washington legislation would have made use of skimmed data for marketing purposes, by a retailer, a civil offense with a fine of up to $10,000 for each violation (however, this provision was dropped from the final bill which was enacted). *Id.* at 1. In 2009, legislation was again introduced in Washington to restrict use of skimmed data for marketing purposes and to require labeling consumer products or packaging that is embedded with RFID technologies. *See* Claire Swedberg, *Washington State Rep Reintroduces RFID Legislation*, RFID J., Jan. 13, 2009, http://www.rfidjournal.com/article/view/4541/. This legislation has not yet been adopted.

document without that person's knowledge or prior consent.[335] The law makes an exception from the definition of this new crime for unintentional reading of RFID tags from identification documents, including unintentionally remotely reading a person's identification document in the process of using RFID in the course of operating a contactless identification document system. Under the exception, it is not a crime to unintentionally remotely read a person's identification document unless the reader thereafter intentionally discloses, stores or uses the personal data derived from the reading without the other person's knowledge and consent. At least in some circumstances, California's anti-skimming law appears to protect consumers from skimming of their identification documents to obtain personal data that could later be used for marketing purposes.[336]

RFID-specific legislation has also been proposed in other states. Proposed legislation is pending in New Hampshire that would require a notification label on any consumer product that contains RFID chips.[337] The proposed legislation would prohibit tracking of individuals by means of remotely readable devices in consumer products, such as RFID tags.[338] The bill also requires a consumer notice for consumer products that include remotely readable devices that states: "This (specify product type) may contain a remotely readable device which can be read without your knowledge if it is brought within range of a reader device."[339] Alternatively, the required consumer notice may be provided by a graphical

---

335. S.B. 31, 2007–08 Cal. Reg. Sess. (adopted Sept. 30, 2008). Identification documents are broadly defined in the bill to mean "any document containing data that is issued to an individual and which that individual, and only that individual, uses alone or in conjunction with any other information for the primary purpose of establishing his or her identity." *Id.* § 1798.795(c). Driver's licenses and identification cards issued by public agencies or private businesses are included in the definition. *Id. See also* K.C. Jones, *California Bans RFID Skimming*, INFORMATIONWEEK, Oct. 2, 2008, http://www.informationweek.com/news/mobility/RFID/showArticle.jhtml?articleID=210605275.

336. S.B. 31 does not appear to apply to the provision of RFID-enabled mobile phones to consumers or reading RFID data from those phones since it only applies to identification documents defined as "any document containing data." S.B. 31, § 2; CAL. CIV. CODE § 1798.795(c) (2008)

337. *See* Heim, *supra* note 332.

338. *See* An Act Relative to the Regulation of Remotely Readable Devices and the Illegal Use of Payment Card Scanning Devices or Reencoders, H.B. 686, 160th Gen. Ct., 2007 Sess. § 358-T:5 (N.H. 2007) (as amended by the House, Mar. 18, 2007), *available at* http://www.gencourt.state.nh.us/legislation/2008/HB0686.html [hereinafter H.B. 686]. In the bill, " 'track' means to locate, follow, or plot the path of an individual by means of a remotely readable device, but shall not include technology used by the enhanced 911 system or commercial mobile radio service pursuant to 47 U.S.C. Section 332." *Id.* § 358-T:1VIII. H.B. 686 was passed by the state House of Representatives and is currently pending in the state Senate. *See* H.B. 686, Advanced Bill Status Search, New Hampshire Legislature, http://www.gencourt.state.nh.us/bill_status/ (last visited Jan. 2, 2009).

339. *See* H.B. 686, *supra* note 338, § 358-T-1.

system designed to provide a standardized way to show the presence of a remotely readable device.[340] The bill's notice requirements for consumer products that include RFID tags are not applicable to locating technologies in which unique identification via radio waves is an essential part of the consumer's use of the product, including technologies used to provide the 911 emergency response system and to provide commercial mobile radio service (e.g., wireless telephone service provided by mobile carriers).[341] If this bill is enacted in New Hampshire, it appears it will not require a consumer RFID notice before sale of RFID-enabled mobile phones. It also would not restrict the use of location tracking technologies by mobile carriers, such as cell phone triangulation or GPS, that are part of providing mobile services to consumers. However, the bill reasonably may be interpreted to restrict direct tracking of consumers with RFID-tagged mobile phones for purposes of delivering LBS and mobile advertising, because this type of tracking does not utilize the location tracking technologies used by mobile carriers in the delivery of services to subscribers. While the Electronic Privacy Information Center (EPIC) supports H.B. 686, it urges revision of the bill to add provisions regulating unique identifiers stored on tags that could be linked to databases containing personally identifiable information and requiring labeling of "RFID readers and interrogators, as well as RFID tags and products containing tags."[342] .

Alaska is also considering proposed legislation to outlaw unauthorized scanning and reading of RFID tags and prohibit providers from requiring continued activation of RFID tags in order for consumers "to exchange, return, repair, or service an item that" contains an RFID tag.[343] This proposed legislation in Alaska also requires providers of RFID-tagged products to give consumers notice of RFID-tags and obtain their

340. *Id.* §§ 358-T:1(III)(a), 358-T:2(II).

341. *Id.* § 358-T:1(II) (defining "consumer product," for purposes of the legislation to require a notice to be affixed to consumer products that a remotely readable device has been affixed or implanted, to exclude "an identification document or any product to the extent that unique identification via radio waves is an essential part of the consumer's use, including, but not limited to, commercial mobile radio service as described in 47 U.S.C. § 332.")

342. EPIC Letter, *supra* note 7 (EPIC's analysis of H.B. 686). H.B. 686 § 358-T:4(II) restricts the use of identification documents permitted under the section from containing, transmitting or enabling "the remote reading of any personal information other than a unique personal identifier number which is not a social security number." H.B. 686, *supra* note 338. EPIC argues that these unique identifiers can be used to create detailed personal profiles of individuals and to track individuals and thus need to be regulated to prevent misuse or abuse. *See also EPIC's Guidelines on Commercial Use of RFID Technology*, *supra* note 172.

343. An Act Relating to Electronic Communication Devices and to Personal Information and Making Certain Violations Related to Electronic Communication Devices Unfair Trade Practices, S.B. 293, 25th Legis., 2008 Sess. §§ 45.48.040, 45.48.060 (Alaska 2008). EPIC testified on the proposed Alaska legislation before the Alaska State Senate.

advance consent before collecting and using their personal information.[344] EPIC analyzed this proposed legislation and recommended four changes including: (1) adding a private right of action so that citizens may directly pursue a remedy; (2) adding stronger consumer deactivation rights so that it shifts the burden from the consumer to the provider to deactivate an RFID device at the consumer's request and to provide an option to consumers for permanent deactivation of the device; (3) adding provisions to cover unique identifiers linked to databases containing personally identifiable information; and (4) requiring labeling of RFID readers and interrogators, as well as RFID tags and products containing tags.[345]

In sum, as of the time of this writing, no state law has been adopted that requires notice and/or labeling of RFID-enabled mobile phones by providers or that regulates m-advertising practices related to the use of RFID-enabled mobile phones.

2. Federal and State Guidelines on Online Marketing Practices

It is a common practice for Web sites to collect data about consumers' Web-surfing behavior and to use that information to help their advertising clients deliver targeted ads to specific consumers, based on their online behavior, demographics and interests.[346] These practices involve consumer profiling, as discussed earlier in this paper.[347] Such targeted marketing practices are not federally regulated in the United States and the Web sites and advertisers are not currently required by law to obtain the consent of consumers before collecting and using this information for targeted marketing purposes (apart from the requirement to comply with their own privacy policies to avoid engaging in unfair or deceptive trade practices that are prohibited by the FTC).[348]

While the FTC has not yet addressed consumer privacy regarding mobile advertising practices that collect data about consumers' behavior using their mobile phones in order to target them with mobile advertising, it has published self-regulatory privacy principles for online marketing practices known as "behavioral advertising" (online behavioral

---

344. *Id.* § 45.48.020; *see also* Top News, *EPIC Urges Alaska Senate to Protect Consumers from RFID Misuse*, EPIC, Mar. 17, 2008, http://epic.org/privacy/rfid/ (last visited Feb. 10, 2009) (discussing Alaska's proposed S.B. 293 on electronic communication devices including RFID technologies).

345. *EPIC Testimony on AK RFID Bill*, *supra* note 108, at 6–9.

346. *See* Louise Story, *A Push to Limit the Tracking of Web Surfers' Clicks*, N.Y. TIMES, Mar. 8, 2008.

347. *See generally* text and references discussing consumer profiling, *supra* Part IV.E.

348. *See supra* Part VII (discussing breach of promises in a privacy policy as an unfair and deceptive trade practice within the FTC's regulatory jurisdiction).

advertising is the practice of tracking consumers' activities online in order to direct target advertising to them). These guidelines recommend that Web sites post a privacy statement and obtain consumers' consent in advance before collecting their data.[349] Consumer groups have urged the FTC to adopt a "do not track" registry that would allow consumers to prevent advertisers from collecting information about them.[350]

At the state level, legislation was proposed (but not enacted) in New York that would require Web sites and advertisers to obtain consumers' consent before collecting and using their personal data for targeted online advertising purposes. This legislation would have made it a crime to violate consumers' privacy rights under the statute.[351] This proposed law also would have regulated practices that can generally be described as consumer profiling.[352] Due to the interstate nature of Internet access, it would be difficult for online marketers to comply with this law by providing privacy protections for people residing in New York but not for residents of other states, but it could encourage Web sites to adopt national privacy standards and practices consistent with the New York law. A trade group representing several large Internet companies opposes the bill and argues that it is most likely unconstitutional.[353] The debate over

---

349. FED. TRADE COMM'N, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 45–47 (2009), http:/www.ftc.gov/os/2009/02/P085400behavadreport.pdf (announcing a set of online behavioral advertising principles to guide self-regulatory practices of companies engaged in behavioral advertising). The privacy principles include: (1) transparency and consumer control; (2) reasonable security and limited data retention for consumer data; (3) affirmative express consent for material changes to existing privacy promises; and (4) affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising. *Id.* Regarding notice and consent, the FTC's guidelines provide: "Every Web site where data is collected for behavioral advertising should provide a clear, consumer-friendly, and prominent statement that (1) data about consumers' activities online is being collected at the site for use in providing advertising about products and services tailored to individual customers' interests, and (2) consumers can choose whether or not to have their information collected for such purpose." *Id.* at 46.

350. Diane Bartz, *Consumer Groups Urge "Do Not Track" Registry*, REUTERS, Apr. 15, 2008, http://www.reuters.com/article/governmentFilingsNews/idUSN1520070020080415; *see also* Grant Gross, *Privacy Advocates: Consumer Education Isn't Enough*, IDG NEWS SERVICE, Apr. 17, 2008, http://www.pcworld.com/businesscenter/article/144756/privacy_advocates_consumer_education_isnt_enough.html (arguing that Congress should pass online privacy regulation including a "do not track" register). Congress held hearings in 2008 to investigate whether there is a need to regulate online behavioral advertising practices to protect consumers' security and privacy. Joelie Tessler, *Microsoft, Google Back Broad Privacy Legislation*, SFGATE.COM, July 9, 2008, http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2008/07/09/financial/f125127D29.DTL (reporting on a Senate Commerce Committee hearing on online advertising).

351. *See* Story, *supra* note 346, at 1.

352. *See generally* text *supra* Part IV.E.

353. *Group Calls Targeted Advertising Bill Unconstitutional*, GIGALAW, Apr. 10, 2008, http://www.gigalaw.com/news/2008/04/group-callls-targeted-advertising-bill.html (citing WALL ST. J.).

whether government regulation is necessary to regulate behavioral advertising practices or if industry should be allowed to self-regulate is likely to be intense and to extend to emerging mobile advertising practices.[354]

VIII. Proposing Self-Regulatory Steps to Address Consumer Privacy Concerns

Apart from the ongoing work on RFID by governments in the European Union and the United States, notable work has already been done by respected organizations to analyze the privacy and data protection concerns associated with commercial use of RFID and to propose guidelines to protect consumers in this context. For example, the Electronic Privacy Information Center (EPIC) published its "Guidelines on Commercial Use of RFID Technology" in 2004.[355] The Organisation for Economic Cooperation and Development (OECD) has also made an insightful contribution to this discussion with its 2007 report: "Radio Frequency Identification (RFID): A Focus on Information Security and Privacy," and has been involved in designing privacy and data protection guidelines since issuing its 1980 OECD Privacy Guidelines.[356] The work of EPIC and the OECD is a good starting point for discussion of needed regulatory reform. EPIC's work articulates consumer privacy and data

354. Renee Boucher Ferguson, *A Battle is Brewing Over Online Behavioral Advertising*, eWeek, Mar. 27, 2008, http://www.eweek.com/c/a/Enterprise-Apps/A-Battle-Is-Brewing-Over-Online-Behavioral-Advertising-Market/. *See* Villoch III, *supra* note 18 (discussing the role of government regulation and industry self-regulation to ensure consumer trust in order to encourage the growth of e-commerce). Those who argue government regulation to protect consumer privacy will unduly restrict the growth of mobile commerce and that mobile advertising will be able to appreciate the industry self-regulatory approaches to protecting consumer privacy are in the next section of this paper.

355. *See EPIC's Guidelines on Commercial Use of RFID Technology*, *supra* note 172.

356. *See OECD Report on RFID*, *supra* note 16, at 41; *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), *available at* http:/www.oecd.org/document/20/0,3343,es_2649_34255_15589524_1_1_1_1,00.html. The OECD fair information practices 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. Ciocchetti, *supra* note 101, at 61 n.26. The OECD is an international organization established in 1961 and composed of thirty member countries committed to democracy and the market economy, which shares expertise and views with one hundred other countries and market economies. *About the OECD*, OECD, http://www.oecd.org/pages/0,3417,en_36734052_36734103_1_1_1_1_1,00.html (last visited Jan. 2, 2009). The United States and many European Union member-countries are also members of OECD. Ratification of the Convention on the OECD: OECD Member Countries, http://www.oecd.org/document/58/0,3343,en_2649_34483_1889402_1_1_1_1,00.html (last visited Jan. 2, 2009).

protection principles that are a foundation for the analysis in this section regarding the commercial use of RFID-enabled phones to deliver LBS and mobile advertising. Similarly the OECD Report on RFID identifies important issues from a general standpoint that need to be resolved in this new specific context.

While it may be unlikely that broad data protection legislation will be adopted in the United States, legislative efforts to regulate the use of RFID in consumer products and targeted marketing practices may be gaining momentum.[357] Although there has been much examination of the use of RFID technologies from the standpoint of privacy and security in the European Union, the European Commission's newly proposed RFID Recommendation is not binding legislation, and instead encourages industry and company self-regulation.[358] Even if new laws are not adopted in the European Union or the United States to regulate RFID-enabled mobile phones and RFID-embedded consumer environments, high levels of protection could be afforded for consumers by conducting privacy impact assessments in the context of RFID-enabled mobile phones to be used in RFID-embedded environments, taking into consideration the usefulness of this application of RFID technologies for the delivery of mobile advertising and other location-based services.

This next section of the paper discusses privacy-impact assessments as a self-regulatory process to be used by companies to identify relevant consumer privacy concerns and possible policy and technical design related to applications of RFID for consumer products like mobile phones. Then, considering the new business context of using RFID-enabled phones to deliver mobile advertising and location-based services, it describes three classes of topics that should be included in privacy impact assessments and provides an example application for each type of classification. Finally, this section provides a list of questions for discussion among legal and technical experts seeking to find privacy-enhancing solutions for the consumer privacy challenges posed by RFID-enabled mobile phones.

A. *The Need for Privacy Impact Assessments*

A privacy impact assessment (PIA) "is usefully defined as a process whereby a project's potential privacy issues and risks are identified and examined from the perspectives of all stakeholders, and a search is

357. *See supra* Part VII.B.
358. *See supra* Part VII.A.2.

undertaken for ways to avoid or minimi[z]e privacy concerns."[359] One of the most significant aspects of the European Union's Proposed RFID Recommendation is its support for conducting PIAs before introducing new products or services based on RFID technology to consumers.[360]

As the OECD Report on RFID emphasizes:

> There is a broad variety of RFID hardware and software configurations deployed in many different contexts. RFID technology does not systematically or inherently generate privacy issues and, when it does, the nature, scope and extent of these privacy issues vary according to both the technology and the use context. In most cases, the potential invasion of privacy through the use of RFID is likely to be proportionate to several interrelated parameters including: (i) a tag's capacity to be read at a distance without the participation of the individual; (ii) the possibility to reveal intrusive or sensitive information about individuals through inferences and profiling; (iii) the degree of interoperability (who can read the tags; who can access the full information about the product); and (iv) the tracking capabilities of RFID.[361]

While technology-neutral regulation is often advocated as an essential regulatory principle in order for governments to avoid adopting regulation that stifles technological innovation, not all uses of RFID present the same privacy and data protection concerns, and the business context and the particular technologies involved are important considerations. Consistent with the OECD's Report on RFID, RFID privacy guidelines should not be one-size-fits-all; rather, the specific privacy risks for consumers should be considered in the context of the RFID technologies being used[362] and privacy-protecting solutions proposed.

The OECD's Report on RFID states that, due to the wide variety of technical configurations and use scenarios, there will be a need to conduct PIAs for new commercial contexts. A PIA should consist of an in-depth examination of whether and to what extent the use of the technology actually gives rise to privacy concerns in a given system and should include: "examining the RFID application, the kind of data collected, the nature and technical specification of the RFID technology

---

359. ICO PIA Handbook, *supra* note 323, at pt.II. A PIA aims to prevent problems from a privacy perspective and is best undertaken at an early stage in a project and is distinguished from a privacy audit (which is after the fact) and from a legal compliance audit. *Id.*

360. *Draft RFID Recommendation*, *supra* note 315, art. 3.1 (privacy and data protection measures should include a privacy impact assessment by application operators).

361. *OECD Report on RFID*, *supra* note 16, at 38.

362. *Id.* at 48.

used and the potential that the collected data will be related to an individual or identifiable individual."[363] The OECD's Report on RFID recommends that the PIA occur early, at the design stage, so that the privacy impact of an RFID system can be identified and best strategies to mitigate privacy risks can be employed.[364] The OECD's Report on RFID further advocates a holistic approach to privacy management that would consider "each stage and each component of the overall system" and "the whole lifecycle of the RFID data within an organization's broader information system."[365]

These PIAs need to be done in the context of providing LBS services and mobile advertising through RFID-equipped mobile phones. The process will necessarily involve technical experts as well as legal and business experts. It is anticipated that businesses and industry-associations, such as global industry associations like the Near Field Communication Forum (NFC Forum), will contribute input to the privacy discussions that need to occur related to this topic.

The NFC Forum is an industry association of global businesses brought together by their support of the development of near field communications technologies and services. The NFC Forum's members include mobile carriers, mobile handset providers and other businesses that are involved in developing applications and providing services to support delivery of LBS and mobile advertising in the context of RFID-enabled mobile phones using NFC technologies.[366] As discussed earlier in this article, the Privacy Advisory Council of the NFC Forum is planning to issue guidance for developing privacy policies related to the use of NFC technology and a privacy checklist detailing for interested parties the privacy tenets associated with using NFC technologies.[367] At the time of this writing, the NFC Forum had not yet published these resources on its Web site, but when they are available, they will need to be examined in light of existing privacy regulation and the need for adequate consumer privacy protections.

---

363. *Id.*

364. *Id.*

365. *Id.*

366. NFC Forum, Members, http://www.nfc-forum.org/member_companies/ (last visited Jan. 4, 2009).

367. *See* NFC Forum, Privacy Advisory Council, http://www.nfc-forum.org/aboutus/committees_and_wgs#pac (last visited Jan. 2, 2009). For a discussion of the NFC's plans to issue privacy guidance in the form of a position paper that addresses policies for protecting privacy when using NFC technology and a privacy checklist, see *supra* note 172 and accompanying text.

B. *Topics for Privacy Impact Assessments*

The process of conducting a PIA should include a consideration of the application of fair information practices in the context of using RFID-enabled mobile phones to deliver LBS and m-advertising.[368] It should also consider privacy-enhancing technologies.[369] Since there is no one-size-fits-all PIA, this article offers three examples of topic categories to include in PIAs related to the use of RFID-enabled phones in delivering LBS and m-advertising, as follows:

1. Implementing Fair Information Practices

The need to provide adequate notice to consumers who will use the RFID-enabled phones in RFID-embedded environments is consistent with the generally accepted fair information practice of notice to consumers.[370] A PIA in this context should consider including the following types of information in consumer notices:

(a) That the consumer's mobile phone is RFID-enabled, including whether it contains a tag, reader, or both and the applicable communication ranges;

(b) Whether the consumer's environment (e.g., shopping center, bus station) is embedded with RFID technologies;

(c) Whether the consumer is being profiled or tracked, by whom, and for what purpose;

(d) Whether data (e.g., personal, profiling, tracking) about the consumer is being collected, used, stored in a data base, shared, etc.;

(e) How long the data are stored, where and by whom, and whether the data has been made anonymous;

---

368. As David Flaharty says:

> Various models exist for privacy impact assessments that can be customised to the needs of any organisation. The essential goal is to describe personal data flows as fully as possible so as to understand what impact the innovation or modification may have on the personal privacy of employees or customers and how *fair information practices* may be complied with.

David Flaherty, *Privacy Impact Assessments: An Essential Tool for Data Protection*, 7 PRIVACY L. & POL'Y REP. 85, 85 (2000), http://www.austlii.edu.au/au/journals/PLPR/2000/45.html (emphasis added).

369. ICO PIA Handbook, *supra* note 323, Privacy-Enhancing Technologies, at pt.II. The ICO PIA Handbook lists three types of privacy-enhancing technologies: (1) means of countering against privacy-invasive technologies; (2) means of providing genuine, untraceable anonymity; (3) means of providing strongly protected pseudonymity. *Id.*

370. *See* text *supra* Part IV.B.

(f) If consumer profiles are used to deliver targeted marketing, how a consumer can learn about the individual or group profiles applied to him and explanation of the contents of those profiles expressed in language that would be meaningful to a typical consumer;

(g) Whether access to location-based services may be accompanied by delivery of m-advertising to the consumer and information about the consumer's ability to control the frequency, type and time of delivery of any m-advertising;

(h) Whether m-advertisers and other parties involved in the specific RFID system have privacy policies, and if so, short notices that include the essential elements of applicable policies along with links to full privacy policies.

There are many considerations to discuss beyond the contents of the notice, including identifying ways to deliver meaningful notice, such as using standardized logos as well as a written notice, providing notice at times relevant to consumer choice and providing notice in a form that can be accessed and displayed on mobile phones.

2. Application of Privacy Enhancing Technologies

In the OECD Report on RFID, general concepts about PETs are discussed, including the design of RFID tags to include features that empower RFID systems and users to control the technology and prevent or mitigate privacy risks. For example, the report suggests that a "kill command" could be included that is initiated by the retailer at the point of sale to deactivate the RFID tag permanently unless the consumer expressly agrees otherwise.[371] Alternatively, the report comments that an RFID tag's antenna could be removed to shorten its read-range, thus turning a longer range tag into a shorter range tag. A shorter range tag may still be read, for example for warranty service. But a shorter range tag poses less of a privacy-risk for a consumer in terms of the possibility

371. *OECD Report on RFID*, *supra* note 16, at 47. *See also Seven Paths to Privacy*, SCI. AM., Sept. 2008, at 37, which offers policy recommendations for government regulation to protect privacy:

> *Regulate the use of RFID tags.* When RFID tags are embedded in a retail product, they should be disabled once the shopper has paid for the product. Even if they store nothing more than a serial number, they enable anyone who carriers such a tag to be followed surreptitiously. If they must remain readable—as in licenses, passports, and the like—their presence should be disclosed to the carrier. If the tags store personal information, including information about time and place, it should be encrypted and the carrier should be warned about its presence.

Id.

that the tag will be read by other parties and perhaps used to track the consumer because the tag is only readable if it comes sufficiently close to RFID readers.[372] The design alternatives described in the above scenarios give consumers the ability to be anonymous by deactivating RFID tags in products they purchase or to minimize the likelihood that RFID tags in their possession will be read after the point of sale unless they are seeking warranty or other assistance.

When this general theory of PETs is applied in the mobile phone context, the parties conducting the privacy impact assessment should consider which types of technical measures will give mobile phone users some effective control over their privacy when mobile phones have built-in RFID tags and RFID readers. Are there specific ways to give users control that relate to the phone's design for use in delivery of location-based services and m-advertising? Those conducting the privacy impact assessment should consider that users of their products may have different views about the desirable level of privacy that they want:

- Some users will want to have the RFID-tags "killed" at purchase and may choose to disable the RFID readers in their phones, perhaps because they do not intend to use them and fear they will be exposed to more mobile spam;
- Others will want to be able to use the RFID-features in their phones in the future, but not all the time (e.g., these users would appreciate an "on/off switch" for RFID-tags and RFID-readers in their phones if it is technically feasible); and
- Still others may want to have (or be neutral to having) the RFID-features on their phones functional all of the time.

Generally speaking, it is technically possible for RFID tags to be "killed" permanently or put into a "sleep" mode from which they can be awakened.[373] One suggestion to preserve the consumer benefits of RFID

372. *Id.*

373. *See* Ari Juels, *RFID Security and Privacy: A Research Survey*, 24 IEEE J. ON SELECTED AREAS IN COMM. 381, 386 (2006). RFID readers can send kill commands to RFID tags that render the tag permanently inoperative. *Id.* To prevent uncontrolled deactivation of tags, the kill command is protected by a PIN (generally a 32-bit code). *Id.* "Killing or discarding tags enforces consumer privacy effectively, but it eliminates all of the post-purchase benefits of RFID for the consumer," such as the ability to return the item without a receipt. *Id.* Alternatively, the RFID tag can be put to sleep, which makes it only temporarily inactive. *Id.* However, this would provide no privacy protection if any RFID reader could wake the tag, so access control mechanisms are needed, such as PINs. *Id.* Controlling the PINs for kill or sleep commands is a difficult task, especially for consumers. *Id.* If the consumer must do this in order to maintain control over his tags, the consumer would need to keep track of them as well as key them in or scan them in order to use them. *Id.* One benefit of having a mobile phone is that the PIN could be transmitted to the mobile phone for use. *Id.*

tags post-sale is to design an RFID tag that is able to store a privacy bit in its memory that is either "on" or "off". When it is "on," the tag cannot be scanned. When it is "off," the tag can be scanned for such purposes as obtaining warranty service or to return the product without a receipt.[374] The "on/off" status of a tag can be changed if the RFID tag is writable by an RFID scanner, but for security purposes, it is recommended that an RFID-tag-specific PIN be required to change the on/off status of the tag.[375] At least conceptually, design features like those described above would enhance the protection of consumers' privacy and give them control over whether or not the RFID tags in their phones can be read by RFID readers in their environments. This topic should be considered in privacy impact assessments for these new types of mobile phones.

Similarly, privacy impact assessments should consider ways to give consumers a choice about whether the RFID readers in their mobile phones are operable. Since an RFID reader must have a power source, such as a battery, in order to operate, presumably disconnecting the battery by turning the phone off will temporarily put the phone's RFID reader out of operation. However, turning the phone off may be impractical for most mobile phone users because it would interfere with their ability to use the phone for other purposes. Furthermore, if the phone's RFID reader is on when the phone is on, the user may want to be able to choose whether or not the reader will read all RFID tags that are detected within its read range. One reason for this concern is that tags in the consumer's environment may contain advertising or links to advertising Web sites, so having an RFID reader in one's phone that reads every tag that it comes into contact with could expose the mobile phone user to unwanted advertising solicitations displayed on their mobile phone.[376] In

---

374. Ari Juels, *RFID Privacy: A Technical Primer for the Non-Technical Reader*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY, A CROSS-DISCIPLINARY CONVERSATION 57, 70 (K. Strandburg & D. Stan Raicu eds., Springer-Verlag 2005). At the time of this writing, no source was found for information about the specific types of privacy enhancing design features have been included in the new RFID-enabled mobile phones that are being tested in consumer trials.

375. *Id.*

376. The RFID technologies that are the basis of Near Field Communications technologies to be incorporated in mobile phones and other consumer devices can be described as enabling technologies that allow one NFC-compliant device to make contact with another NFC-compliant device by touching each other or coming close to each other, "typically within a few centimeters." INNOVISION RESEARCH & TECHNOLOGY PLC, *supra* note 60, § 4 (describing how NFC-enabled mobile phones can obtain information from NFC-compliant smart posters by bringing it close to or touching the poster with their phones, for example, and thereby access a few lines of text or a Web link).

According to Innovision:

> For two devices to communicate using NFC, one device must have an NFC reader/writer and one must have an NFC tag. The tag is essentially an integrated

the case of RFID-enabled mobile phones that utilize Near Field Communications technologies, it does not appear that the user has any control over whether his phone will read RFID tags in his environment other than to avoid coming within the read-range.[377] Although, at present, this read range may be short and there may be few smart posters or other NFC-compliant tagged items in consumers' environments to be read, this will change as the technology is adopted for many business applications.[378] Receiving advertising by virtue of reading it with one's mobile phone may not technically be spamming in the sense that spam is generally defined as unsolicited advertising. Perhaps it should be categorized as permissive-based advertising assuming the user's RFID reader has initiated the sending of mobile advertising to the phone by interrogating the RFID tags that contain the advertising content. On the other hand, if the tags in the smart posters are capable of initiating contact with the consumer's mobile phone, then this distinction becomes less clear.[379] Such advertising is likely to be unwelcome if there is no way for the user to avoid reading advertising on RFID-tags simply by coming into their proximity.

Another question that needs to be addressed from a technical standpoint is, can users selectively control which RFID readers in their

---

> circuit containing data, connected to an antenna that can be read and written by the reader. There are two modes of operation covered by the NFC protocol: active and passive. In active mode, both devices generate their own radio field to transmit data. In passive mode, only one device generates a radio field, while the other uses load modulation to transfer data. The NFC protocol specified that the initiating device is responsible for generating the radio field in this case. The passive mode of communication is very important for battery-powered devices like mobile phones and PDAs that need to prioritize energy use. The NFC protocol enables such devices to be used in power-saving mode, so that energy can be conserved for other operations.

Id. at 5.

377. *Id.* For insights into which NFC-enabled device controls communications between two NFC-enabled devices, *see id.* § 2.3. NFC-enabled devices are configured to enable the NFC-enabled reading device to initiate communication between two NFC-enabled devices that are in close proximity to each other without the necessity of operator action (except to authorize payment transactions). There is apparently no "on/off" feature that gives the operator of a NFC-enabled device that is being read by another NFC-enabled device control over whether such communication may be initiated by a reading device.

378. *Id.* at 7 (listing "[o]ther devices and equipment likely to become NFC-enabled in the near future [to] include: cash registers and other point-of-sale equipment; cash machines; posters, street signs, bus stops and points of interest; vending machines and parking meters; turnstiles, entry systems and door openers; and product packaging.").

379. Active RFID tags are able to initiate contact with an RFID-reader because they have access to a power source, as opposed to semi-active or passive tags which cannot initiate contact with an RFID-reader. Weis, *supra* note 5, at 978. The power source of an RFID tag "will determine a tag's potential read range, lifetime, cost, and the kinds of functionalities that it may offer." *Id.*

environments are permitted to read the RFID tags in their phones? For example, in the BART-RFID Trial discussed earlier in this article, users must push one button or enter a pin code to activate contactless communications for payment of transit fares.[380] But will a similar control feature, such as a "disable RFID tag"/off-button, allow users to decide whether other RFID readers that have been embedded in a shopping mall or other environment may be allowed to detect their presence through the process of reading the RFID tags in their phones? Passive RFID-tags generally broadcast information stored on the tags whenever they come into the read range of an RFID-reader (essentially they have no "on/off" switch) and they may respond to interrogation by readers without alerting the person who is carrying the device.[381] If the RFID tags included in mobile phones lack an "on/off" switch, a technical solution will need to be found to address this privacy concern.[382]

3. Implementing Privacy Enhancing Technologies That Enhance Transparency

Labeling RFID-readers in shopping malls and subways is consistent with the fair information practice of notice because it alerts consumers that their personal information and privacy may be at risk if they have RFID-equipped phones with them. Alternatively, PETs that provide notice could be designed, such as designing phones to alert their owners they are within the read range of RFID-readers. Such PETs would serve the purpose of making the components of RFID systems more transparent so that consumers can take steps to protect their privacy and personal information. Transparency is needed by consumers because the nature of the technology is to work silently in the background without the need for human interaction. If this technology creates privacy risks and nothing is done to alert consumers of the risks, they may go unnoticed by consumers.

As discussed earlier in this article, there is also a pressing need to consider transparency enhancing technologies to address the privacy implications of consumer profiling.[383] This section considers some of the privacy concerns associated with profiling. Of particular importance is

---

380. *See supra* text accompanying note 78 (discussing action required by mobile phone user to intitiate payment).

381. *See* Juels, *supra* note 373, at 382.

382. *See* Mark Roberti, *Zhenuine Introduces Consumer-Controllable Tag, Online Registry*, RFID J., Jan. 28, 2009 (announcing that a startup firm has developed a method for making radio frequency transponders that communicate with interrogators only when a person activates the tag by pressing a button on it, enabling consumers to prevent others from reading information on tags they hold without their consent).

383. *See* discussion of the privacy implications of profiling for targeted marketing purposes, *supra* Part V.E. *See generally* Dinant et al., *supra* note 13.

the use of profiling as part of a system to deliver targeted location-based services and targeted m-advertising and the possibility of addressing these privacy concerns through the employment of PETs designed to provide transparency to consumers. For example, it has been suggested that in order to make consumer profiling practices more transparent, consumers should be given access to information about the classifications applied to them for this purpose.[384] PETs designed to provide transparency have been described as transparency-enhanced technologies or TETs.[385] This topic is particularly appropriate when considering industry and company self-regulation in the current context. This is because there are no clear legal obligations for companies to give consumers access to the group profiles that are being applied to them by marketers or businesses delivering location-based services, especially when those classifications are based on anonymous data and no personal data are being used or generated.[386] Arguably, consumers have an important privacy interest in gaining access to profiling information in order to better understand how the application of these profiles is affecting their lives. Access to this type of information is essential in our society in order to exercise personal autonomy and individual freedom.[387] Practically, such access may also influence the discussion of whether legal regulation of targeted marketed practices is needed.

C. *Other Privacy Questions That May Have Technical Solutions*

This section outlines RFID-specific privacy questions and possible technical solutions that relate to RFID-enabled phones used in RFID-embedded environments for delivery of LBS and mobile advertising. These questions were revealed by the study conducted for this paper and are based on discussions with technical experts and a review of literature regarding protecting users' privacy and security with respect to RFID technologies.[388] These sources support the conclusion

384. *See supra* Part V.A (referencing the work of Mireille Hildebrandt on transparency-enhancing technologies).

385. *Id.*

386. Although there appears to be no current basis in U.S. law to argue that there is a legal obligation to disclose this information, there is some basis to argue that E.U. law may make the use of classifications for this purpose unlawful, at least without the consent of the affected consumers. *See* discussion on Article 15 of the Data Protection Directive, *supra* note 140; *see also supra* Part VII.B.2. for discussion of developments in U.S. law about the need for privacy protections related to online behavioral advertising practices that could lead to legislation to protect consumers in this context. *See generally* Dinant et al., *supra* note 13.

387. *See* discussion *supra* Parts V.E., VI.A.

388. *See generally* Gildas Avoine, *Bibliography on Security and Privacy in RFID Systems*, UNIVERSITÉ CATHOLIQUE DE LOUVAIN, LOUVAIN-LA-NEUVE, BELGIUM, May 18, 2008, http://www.avoine.net/rfid/; Juels, *supra* note 112 (discussing solutions for problems of authentication and privacy regarding RFID); Juels, *supra* note 373, at 381 (providing a survey of

that, at least theoretically, there are technical solutions for many of the perceived privacy concerns related to RFID-enabled mobile phones. The list is offered to stimulate discussion among privacy experts with technical and legal backgrounds who can hopefully work together to find privacy-enhancing solutions to adequately protect consumers' privacy in the era of RFID-enabled mobile phones, location-based services and mobile advertising. To the extent that such solutions are found, it will reduce the need for RFID-specific government regulation that could discourage further development of new and useful location-based services using RFID technologies and create legal barriers engaging in global mobile commerce.

(1) Is it technically possible to give a consumer the ability to temporarily disable the RFID tags and RFID reader in his mobile phone? Yes, it is theoretically feasible to include an "off switch" allowing a user to temporarily or permanently disable the RFID features of his phone after purchase. One way to do this would be to connect the RFID-tag and the RFID-reader in the user's mobile phone to the electronic system in the phone, thus enabling the user to control whether the RFID-tag and RFID-reader are active by pushing a button to disable these features.[389] Another approach would be to include a switch in RFID tags used in mobile phones that prevent the RFID tags from being read by RFID readers unless the phones' users activate the tags by pushing a button.[390]

(2) Is it technically feasible to design an RFID-enabled mobile phone that will allow the user to release part of the informa-

---

technical research on the problems of privacy and security for RFID); Juels, *supra* note 374; Ari Juels & Stephen Weis, *Defining Strong Privacy for RFID*, CRYPTOLOGY EPRINT ARCHIVE, Report 2006/137 (2006) http://eprint.iacr.org/2006/137.pdf; Henrik Granau, *Design patterns and Business Models for a New Generation of RFID Solutions*, RFIDSEC (Dec. 11, 2007), http://www.rfidsec.com/docs/RFID%202.0%20article%2012-11-2007.pdf (discussing the new generation of RFID Solutions, RFID 2.0).

389. These conceptual design proposals are based on discussions among legal and RFID experts at a meeting at Université Catholique de Louvain, Louvain-la-Neuve, Belgium held in May 2008 [hereinafter Meeting to Discuss Privacy-Enhancing Design Features for RFID-Enabled Mobile Phones]. Any errors in describing these possible technical design features and the underlying technology remain the author's own.

390. *See* Roberti, *supra* note 382 (reporting that a start-up company recently announced that it had developed a mechanical switch for passive RFID-tags that will put the tag's owner in control of whether information on the tag can be read by RFID-readers). The "tags can be used in driver's licenses, passports and even individual items to protect the consumer's privacy." *Id*. (quoting Denny Choi, president of Zhenuine, the company that developed the new switch for RFID tags).

tion stored on his phone (like his contact information) to an advertiser or other business (like a friend-finder service) while keeping other parts of the information stored on his phone private? Yes, at least theoretically because the information stored on a mobile phone is stored in computer memory and computer memory may be partitioned so that different access restrictions can be put on different components of computer memory. There are at least two types of memory on RFID-enabled mobile phones—the memory storage on the RFID chips in RFID tags embedded in the phone and the memory storage on the phone itself that allows the user to store his contact list. Both types of memory storage could be partitioned to impose access restrictions, giving the user the ability to control access to some of the data stored on his phone and protecting other data stored on his phone from unauthorized access. This feature would be particularly helpful to give the user control over whether to release his personal information and the contact information for other people stored on his phone that is included in his contact list. Similarly, to the extent that the RFID tag in his mobile phone contains personal and non-personal information, the ability to partition the memory on the RFID tag and control access to the different parts of the memory would enable the user to control access to his personal information. For example, the user could release his unique identifying number for the phone that is stored on the phone's RFID tag, perhaps to get warranty service for the phone, while protecting other personal information stored on the tag, such as his mobile phone number.[391]

(3) Is there a way to use database technology linked to the Internet to enhance the transparency of RFID systems designed to interact with consumer devices like RFID-enabled mobile phones? Yes, in theory, each consumer could be provided with an individual online account that she can access in order to review the personal data that a business has collected and used to deliver mobile advertising and other location-based

391. *Id.* Encryption can be used to protect data stored on the user's phone. *See* Albrecht, *supra* note 7, at 74 (discussing the encryption features of RFID tags designed using the ISO 14443 standard and the need to crack the encryption to read data from an ISO 14443 chip).

services to her.[392] Individual online accounts could also be used by marketers to give a consumer access to the individual or group classifications or profiles that have been constructed in order to generate targeted advertising and other promotions to her as part of its customer relationship management strategies.[393]

(4) Is there a way to make use of a passive RFID-tag anonymous, so that it will not reveal any personally-identifying information about the user? Yes, the passive RFID chip in the user's mobile phone could certainly be used to store only information that is not personal information, such as a unique identification number for the phone, but not the user's mobile phone number, name, etc.[394] Even if personal information is stored on the RFID-tag in the user's mobile phone, theoretically a process of encryption could be used in conjunction with the RFID-tag so that the personal information that is stored on the tag will not reveal any personal information to an outsider who skims the information on the tag unless the outsider also has access to the encryption key.[395] However, even when information on an RFID tag is encrypted, it can be used to track or profile a consumer since the encrypted data still provides a unique reference for the mobile phone that can be used for tracking or profiling.[396]

(5) Is there a technical way to prevent consumer profiling of a mobile phone user that is otherwise made possible due to hav-

---

392. *See* Cleff & Gidofalvi, *supra* note 38, at 273 (suggesting the creation of personal data accounts for each user in a secure system that limits access to the personal data of a certain user, perhaps by means of a digital signature).

393. Meeting to Discuss Privacy-Enhancing Design Features for RFID-Enabled Mobile Phones, *supra* note 389.

394. *See* Juels, *supra* note 373, at 382–83 (commenting that "most RFID tags emit unique identifiers . . . [but] the threat to privacy grows when a tag serial number is combined with personal information.").

395. *Id.* at 385 (categorizing RFID tags as "basic tags," meaning those that cannot execute standard cryptographic operations like encryption, and "symmetric-key tags", those that are able to perform symmetric key cryptographic operations and cost more than basic RFID tags).

396. *See id.* at 382–83. This report explains why RFID tags that contain encrypted data can still be used for tracking:

> Most RFID tags emit unique identifiers, even data with cryptographic algorithms . . . . In consequence, a person carrying an RFID tag effectively broadcasts a fixed serial number to nearby readers; providing a ready vehicle for clandestine physical tracking. Such tracking is possible even if a fixed tag serial number is random and carriers no intrinsic data. *Id.* at 382–83.

ing an RFID-equipped mobile phone? Yes, it is theoretically possible to design RFID-tags to emit a different identification number, for example, a randomly generated number, each time they are accessed in order to prevent a party that is reading the tag from identifying the phone as the same phone that has communicated with an RFID-reader on previous occasions. Although profiling for customer relationship purposes can be accomplished without knowing the identity of the mobile phone user, it is not possible to track a consumer with an RFID-enabled mobile phone if his phone emits a different identifier each time an RFID reader detects the phone's presence. So, it is possible to give consumers' control over whether their RFID-enabled phones permit profiling by marketers by designing software for mobile phones that will give consumers the ability to use their phones without having their phones emit a constant unique identifying number, e.g., by generating a different random number whenever the phones communicate with RFID readers such as those in shopping malls or transit centers.[397]

(6) Is standardization of mobile phone design occurring in the case of RFID-enabled mobile phones so that the same privacy-enhancing design features will be included in phones used by both E.U. and U.S. consumers? Yes, there are industry-led efforts to standardize the design of RFID applications for mobile phones in order to achieve the goal of making mobile phones interoperable with RFID systems around the world. For example, Near Field Communications (NFC) technologies are being developed by the Near Field Communication Forum.[398] NFC technologies incorporate RFID into the design of mobile handsets, software for mobile phones and other components of RFID systems that will enable businesses to communicate with these phones to deliver mobile advertising and other location-based services.[399] There is a great opportunity for the NFC Forum (or another similar industry consortium focusing on RFID technologies for mobile phones) to include standardized technical design features

397. Meeting to Discuss Privacy-Enhancing Design Features for RFID-Enabled Mobile Phones, *supra* note 389.

398. *See* discussion of the NFC Forum, *supra* Part VI.B.

399. *Id.* As discussed earlier, the NFC Forum is the leading global consortium of industry players involved in this effort and includes handset manufacturers, software designers, and mobile carriers that are all working together to achieve the goal of interoperability of NFC technologies in consumer devices. *Id.*

> to protect consumers' privacy and personal data in the NFC technologies being developed to incorporated into RFID-enabled mobile phones and RFID-embedded consumer environments. The challenge for the NFC Forum is to develop privacy-enhancing technologies for RFID-enabled mobile phones. If it does so, it will be able to make a significant contribution to finding global privacy solutions. Due to the difficulty of legislating global privacy solutions, standardization combined with development of privacy-enhancing technologies will provide more consistent global privacy protections for consumers in this new business context than could be achieved through government regulation that would likely differ from country to country.

Conclusion

The evaluation of consumer privacy presented in this article is the starting point for discussions that need to take place among relevant industry leaders, government regulators and technical experts as they take on the important task of addressing consumer privacy concerns regarding the implications of RFID-enabled phones, mobile advertising and other location-based services. Due to the global nature of mobile commerce and the opportunity for mobile advertising and location-based services to be offered to consumers no matter where they live, there needs to be international cooperation to identify global solutions to support the growth of mobile commerce—solutions that will both protect personal privacy interests and establish a framework for businesses that is predictable and workable for global transactions. It is critical for companies, industry associations and government regulators to engage in privacy impact assessments that address the RFID-specific implications of new mobile phone technologies. Industry leaders like the Near Field Communications Forum are uniquely poised to provide leadership in the effort to find and adopt privacy-enhancing technologies and practices that will protect consumers in the era of RFID-enabled mobile phones.

It is too soon to tell if current efforts at industry self-regulation will be successful. If industry self-regulation responds to the privacy challenges of RFID and adopts privacy enhancing technologies and policies that give consumers the tools and knowledge they need to take an active role in their own privacy protection, the role of government regulators may be able to be limited to regulatory oversight. Such oversight should be focused on the important consumer protection role that is now provided by governments in the European Union and the United States. This

vision of successful industry self-regulation is certainly rosy and indicates a future for mobile commerce that is bright for mobile advertisers, businesses that provide other location-based services and the RFID industry. This scenario is equally bright for consumers who will reap the benefit of new location-based services and relevant advertising, while having their privacy adequately protected.

Failure of industry self-regulation in this new business context would come at considerable risk to consumers' privacy. It would lead to the potential abuses described earlier in this article and the likelihood that RFID-specific regulation will be adopted in both the European Union and the United States. Compared to the United States, the European Union seems poised to intervene by imposing binding RFID-specific regulation should industry self-regulation fail to protect consumers' privacy. Should the European Union decide to actively regulate RFID technologies and the United States fail to do so, this would create a regulatory imbalance that would have negative ramifications for the growth of global mobile commerce.