



Wireless Location Privacy: A Report on Law and Policy in the United States, the European Union, and Japan

Linda Ackerman, James Kempf

DoCoMo USA Labs
181 Metro Drive, Suite 300
San Jose, CA, 94043
USA

kempf@docomolabs-usa.com

Toshio Miki

NTT DoCoMo
3-5, Hikarinooka,
Yokosuka-shi,
Kanagawa, 239-8536
JAPAN

miki@mml.yrp.nttdocomo.co.jp

October 28, 2003

ABSTRACT

This paper discusses current developments in the law and regulations governing the use of wireless location information in the United States, the European Union, and Japan. Third-generation (3G) telephones that will soon be available are able to send and receive far larger data packets than previous models, enabling the transmission not only of large text files, but also of digital photos, audio, and video. Network Address Translation (NAT) technology is increasing the address space with IPv4, and even more address space will become available when IPv6 is widely deployed.

In view of the opportunities these developments present for the growth of location-based services and mobile commerce via cellular telephone it is important to know what the requirements are for the use of wireless location information in major areas of the global market, particularly what form of subscriber consent is required.

The purpose of this paper is to present a clear picture of the regulations and the role they have played so far in the development of wireless location-based markets, as well as the role they will continue to play in the immediate future.

TABLE OF CONTENTS

1	Introduction	3
2	Introduction: Summary of U.S. Location Regulation.....	4
2.1	Opportunities and Issues	4
2.2	The Telecommunications Act of 1996	5
2.3	The 1998 Federal Communications Commission CPNI Ruling	5
2.4	U.S. West v. FCC	6
2.5	The Wireless Communication and Public Safety Act of 1999	6
2.6	FCC Clarification Order on CPNI.....	6
2.7	Final FCC CPNI Ruling.....	7
2.8	The Cellular Telephone and Internet Association’s Request to the FCC to Establish Fair Location Information Practices	7
2.9	The Regulatory Status Quo on Location Information.....	8
2.10	Legislation in the 108 th Congress.....	8
2.11	State Laws Concerning Wireless Location Information.....	8
2.12	State DMCA Laws	9
2.13	U.S. Conclusions.....	9
SECTION 2: WIRELESS LOCATION PRIVACY IN THE EUROPEAN UNION.....		11
3	Introduction: Data Protection in the European Union	11
3.1	Organization for Economic Cooperation and Development Data Protection Guidelines.....	11
3.2	The 1995 Data Protection Privacy Directive	11
3.3	The 1997 Telecommunications Privacy Directive	12
3.4	The 2002 Directive on Privacy and Electronic Communications	12
3.4.1	Location Information, or Localization.....	12
3.4.2	Data Retention	13
3.5	Implementation of the Directive on Privacy and Electronic Communications.....	13
3.6	Status of Implementation of the Directive in EU Member Countries.....	13
3.7	EU Conclusions	17
SECTION 3: WIRELESS LOCATION PRIVACY IN JAPAN		17
4	Introduction: Privacy Law in Japan.....	17
4.1	Constitutional Privacy.....	17
4.2	Protection of Computerized Personal Data Held by the Government	17
4.3	The Personal Data Protection Law.....	18
4.4	How the Personal Data Protection Law Affects the Business Sector.....	18
4.4.1	The Personal Data Protection Law and Wireless Location Information.....	19
4.5	Guidelines on the Protection of Personal Data in Telecommunications Business	19
4.6	Japan Conclusions.....	20
5	General Conclusions.....	20
	Notes.....	21
	Sources.....	27

1 Introduction

Location-based services are applications that make use of information about where a communication device is located. In the area of wireless communications, such applications enable mobile commerce, which presents a major new market for the telecommunications industry. In the United States, the European Union, and Japan, mobile telephones are required by law to be able to provide a subscriber's location within a reasonably close range for emergency purposes. Developing the infrastructure for a mobile location-based emergency response system, including both hardware and software, is taking longer than anticipated. This has caused corresponding delays in creating a mobile commerce market in the U.S and Europe; Japan has made far greater progress and is currently the world leader in mobile commerce.

Meanwhile, a system of regulations governing the use of location information is gradually coming into effect in countries that represent the major markets for mobile communications. It is clear that highly sensitive personal information such as a wireless subscriber's changing location needs protection against misuse by governments and businesses alike. So far, laws and rules of varying clarity, which offer different degrees of protection, have been or are in the process of being enacted in the United States, European Union, and Japan. The purpose of this paper is to survey the status of location data laws and regulations in these parts of the world. It is hoped that this information will serve as a guide for business development.

The research for this study was done on the Internet and through personal interviews with individuals with professional knowledge of the field. Those contacted work for government agencies that regulate telecommunications and privacy, for telecommunications companies, or for nonprofit organizations that deal with privacy issues. All source information is footnoted and included in the Sources section at the back of the paper.

The report concludes that clear guidelines concerning the use of location information are essential for businesses to move confidently into location-based services and mobile commerce. Ambiguous rule-making by the U.S. Federal Communications Commission (FCC), the government agency responsible for regulating the telecommunications industry, may be one factor that is impeding the growth of mobile commerce. In the European Union, the 2002 Directive on Privacy and Electronic Communications, due to be implemented by member countries by October 31, 2003, is one of a package of initiatives intended to create a uniform regulatory framework for the growth of electronic communications throughout the European market. The Directive sets a clear standard of consent for the use of location information, which member countries must follow, although the method of obtaining consent is left up to their regulatory discretion.

In Japan, the 1998 "Guidelines on the Protection of Personal Data in Telecommunications Business," issued by the Ministry of Posts and Telecommunications, promulgate a clear standard of informed consent by a subscriber before location information can be used. These Guidelines have played a significant role in Japan's current pre-eminence in the use of location-based services, along with other strong government initiatives to make the entire country a networked society. While it seems unlikely that the process of implementing the new Personal Data Protection Law passed by the Diet in May 2003, which will codify the Guidelines and create an enforcement structure, will slow the growth of mobile commerce, the imposition of the new law may have consequences that are difficult to predict at the outset.

The paper is organized by country. Background information leading up to promulgation of the current laws or regulations on location privacy is presented first, followed by a discussion of the

present status quo. In the case of the EU, the overall Directive on Privacy and Electronic Communications is discussed first and then its implementation status in individual member countries is presented in a table format. The history and status of regulation of mobile location information is presented next. The paper concludes with a discussion of the impact of the regulations in the U.S., EU, and Japan on the present and future development of mobile commerce.

SECTION 1: WIRELESS LOCATION PRIVACY IN THE UNITED STATES

In this section, we discuss the current state of U.S. law, regulation, and policy regarding location information in depth, and look at pending federal legislation related to location issues. We also consider the effects of state laws, including passage of versions of the Digital Millennium Copyright Act (DMCA) by a number of states. We consider effect U.S. regulations are having now on the growth of location-based services, and may have on their future development.

2 Introduction: Summary of U.S. Location Regulation

The complex and protracted interplay between wireless location legislation or regulation and its implementation is ongoing. It is accurate to say that the rules now governing the use of location information in the U.S. are somewhat muddled, although it is clear that in the private sector at least some form of customer consent is required. It is also clear that only location information derived from provision of a telecommunications service, such as a cellular telephone, is protected to any degree. Location information derived from mobile information services such as wireless Internet access and email, or from global positioning services (GPS), other than automatic car crash notification, is not covered by existing location regulatory policy. Another form of location information that is barely even on the regulatory radar is that generated by an upcoming technology known as RFID—radio frequency ID tags—touted as the answer to inventory control and shoplifting, but carrying the potential of tracking individuals wearing or walking around with products that have embedded RFID tags.¹

This section of the paper analyzes the status of current regulatory policies in the private sector against the background of their evolution through legislation, administrative rule-making, and judicial decisions.

2.1 Opportunities and Issues

With more than 150 million cellular telephone customers in the U.S (increasing at the rate of more than 45,000 daily)² the ability to deliver the Internet, email, and many other services opens a vast arena of commercial possibilities for information services, product sales, and advertising. Although many types of location-based services are already available in Japan, they have barely been introduced in the U.S., partly because cellular hardware makers have required more time than anticipated to implement location-finding technology and also because of continuing ambiguity in the regulations that apply to the control and use of location information.

Location-based services, in addition to emergency police, fire, rescue, and medical assistance, could include weather reports, street and highway directions, transportation schedules for everything from buses to airplanes, movie theater locations and schedules, concierge services, directions to the nearest desired service (no-fee ATM, parking garage, hospital, Italian restaurant, dry cleaner), and the ability to find friends³—as well as employees and aged parents. Location information could be the basis of intelligent transportation systems to help improve the flow of

traffic. Location data could also make possible the delivery of targeted advertising, personalized services, and much more. Certainly, the advantages of an easily portable, information-rich, mobile connection to the Internet cannot be overstated.

Along with delivery of services, location technology offers businesses the possibility of collecting information that could allow them to leverage the delivery of location information (location, plus service or data accessed) along with services and data to market additional services and products. But just as location capability offers almost unlimited possibilities for convenient access to information, services, and people, it also raises the specter of constant commercial tracking and, more ominously, surveillance by government⁴ or private individuals. Adding real-time location to the personal information profiles already collected by many Internet Web sites further undermines the ability of individuals to control the collection and use of their personal information. It further impinges on the much-eroded right, famously articulated by Samuel Warren and Louis Brandeis, to be left alone.⁵

It should not be difficult to understand why location information must be protected and should not be used without meaningful, affirmative consent. The possibility that location data could become part of the stream of personal information in which we have “no reasonable expectation of privacy”⁶ once it has been relinquished—as it arguably is in a service relationship—to a telecommunications carrier or wireless service provider, should give anyone who values their anonymity pause, whether or not they believe they have anything to hide.⁷

2.2 The Telecommunications Act of 1996

The Telecommunications Act of 1996 (the Act) includes location information in its definition of Customer Proprietary Network Information (CPNI), or personal information about a telephone subscriber.⁸ Before the Act added customer location information, CPNI was generally all the information included on a phone bill: time, date, and duration of a call, and number dialed. Prior to the Act’s passage, telecommunications companies were not restricted from selling this information to third parties for marketing purposes.

The Act limits the use of CPNI: “Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of the telecommunications service from which such information is derived, or services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.”⁹

In other words, carriers may use location information to complete the call, but not for any other purpose, such as marketing.¹⁰ What is not clearly specified is the form of customer consent required for a telecommunications service provider to use location information, or when and how consent is to be obtained.

2.3 The 1998 Federal Communications Commission CPNI Ruling

It is the business of Congress to make laws governing telecommunications and the business of the Federal Communications Commission (FCC) to make rules to implement them. Before passage of the Wireless Communication and Public Safety Act (WCPSA, discussed in Section 2.5 below) added the requirement of a customer’s “express prior authorization” for the release of location

information, the FCC decided in February 1998, that Congress intended Section 222(c)(1) of the 1996 Telecommunications Act to mean that a carrier had to “obtain customer approval to use, disclose, or permit access to CPNI to market to a customer service to which the customer does not already subscribe to from that carrier.”¹¹ It concluded that carriers could obtain customer approval by “written, oral, or electronic means”¹² and that notification of the company’s information collection and use policy is required for informed approval.¹³ In response to comments submitted in the rule-making process, the FCC stated that notice and opt-out were not sufficient for informed consent and “express approval,”¹⁴ which was taken to mean a requirement of notice and opt-in consent based on the “total service approach.”¹⁵ That is, CPNI obtained to provide telecommunications services could be used only for that purpose; use for any other purpose requires customer consent.¹⁶

2.4 U.S. West v. FCC

U.S. West (now Qwest), along with other telecommunications carriers and interest groups, challenged the FCC’s 1998 CPNI Order, arguing to the Tenth Circuit Court that the notice and opt-in approach violated the First and Fifth Amendments of the U.S. Constitution.¹⁷ In June 2000, the court agreed, vacating the FCC’s regulations and holding that the “opt-in” approach was not narrowly tailored and that the FCC had failed to adequately consider the less restrictive “opt-out” approach proposed by the telecommunications industry.¹⁸ While the ruling does not specifically endorse the opt-out standard for consent it does seem to say that the opt-in standard is too broad and that it impinges on a carrier’s commercial speech and property rights. In giving commercial speech precedence over individual privacy rights in personal information, the decision appears to set an implausibly high standard for opt-in consent to the use of CPNI.¹⁹

2.5 The Wireless Communication and Public Safety Act of 1999

With the passage of the Wireless Communication and Public Safety Act (WCPSA or E911 Act), Congress began the still unfinished process of creating a national communications infrastructure for emergency services, with 911 as the universal emergency number.²⁰ The WCPSA also amends Section 222 of the Telecommunications Act of 1996 to require wireless service carriers to provide the location information of cellular 911 callers.²¹ And, although it was enacted after the U.S. West decision, which leaned heavily in the direction of endorsing opt-out customer consent to the use of CPNI (section 2.4, above), Section 222(f) of the WCPSA specifically calls for “express prior authorization of the customer [for] the use or disclosure of . . . call location information”²² for non-emergency purposes. This obvious contradiction has yet to be fully clarified by FCC rulemaking.

2.6 FCC Clarification Order on CPNI

The FCC’s response to the *U.S. West* decision (but not to the WCPSA) was its September 7, 2001, CPNI Clarification Order. The FCC found that the court had “analyzed only the constitutionality of the Commission’s interpretation of the customer approval requirement [the ‘opt-in approach’]”²³ Thus, its ruling “applied only to Section 64.2007(c),²⁴ the only provision inextricably tied to the opt-in mechanism . . . [t]he remainder of the Commission’s CPNI rules remain in effect.”²⁵

Where did this leave telecommunications carriers as far as obtaining consent for the use of CPNI? As the FCC states, “we no longer mandate an opt-in mechanism.”²⁶ Further clouding the consent issue, the Commission stated that pending resolution of its Second Notice of Proposed

Rulemaking (NPRM) on CPNI, carriers could, with proper notice,²⁷ use either an opt-in or opt-out consent mechanism.²⁸ Not surprisingly, this has left carriers feeling uncertain of how to proceed.

2.7 Final FCC CPNI Ruling

On July 16, 2002, the FCC reaffirmed the uncertainty over the CPNI consent mechanism in its Third Report and Order and Third Further Notice of Proposed Rulemaking.²⁹ The Commission dealt with the Tenth Circuit's *U.S. West* decision, which effectively vacated opt-in consent as unconstitutional, by deciding on a dual opt-in/opt-out system. That is, the "[u]se of CPNI by carriers or disclosure to their affiliated entities providing communications-related services, as well as third-party agents and joint venture partners providing communications-related services, requires a customer's knowing consent in the form of notice and opt-out approval. Carriers have the choice to use either opt-in or opt-out in this context. Disclosure of CPNI to unrelated third parties or to carrier affiliates that do not provide communications-related services requires express customer consent, or opt-in approval."³⁰

On the one hand, notice and opt-out are required for the use of location information; on the other hand, either opt-in or opt-out will do. Not surprisingly, this ambiguous ruling has left telecommunications carriers uncertain about what kind of consent is needed to use customer location information.

One other significant—and, fortunately, clear—element of the ruling is that it specifically declines to pre-empt states from regulating the use of CPNI. The Commission states that it will continue its practice of using its pre-emption authority on a case-by-case basis.³¹ A later section in this paper (section 2.11, below) discusses regulations concerning location information and location services that have been enacted by various states.

2.8 The Cellular Telephone and Internet Association's Request to the FCC to Establish Fair Location Information Practices

The Cellular Telephone and Internet Association (CTIA) believed that location information was too important to be bundled with other CPNI. Accordingly, in November 2000, it petitioned the FCC to promulgate separate rules on the implementation of fair location information practices for the cellular telecommunications industry.³² It asked that the rules specify (1) prior notice to consumers of location information collection and use; (2) a meaningful opportunity to consent to the collection and use of location information; (3) assurances of security and integrity of the information collected; and (4) technology-neutrality to meet consumers' privacy expectations regardless of the mobile device or location-based service.³³

On July 24, 2002, the FCC released an order declining to issue rules on fair location information practices.³⁴ It found that Section 222(f) of the E911 Act³⁵ had directed carriers to "obtain a customer's 'express prior authorization' before using or disclosing wireless location information, and thus made clear the authorization process for a key element of consumer privacy, [that] no rules are necessary because the statutory language is unambiguous, imposing clear legal obligations and protections for consumers."³⁶ This contradicts the already confusing statement in the Third Rule and Order issued just a week earlier, which specifies notice and opt-out, but permits location service providers to use either opt-in or opt-out. The Commission also found, despite many comments to the contrary, that Congress had not required it to make rules on Section 222(f) of the E911 Act.

2.9 The Regulatory Status Quo on Location Information

The combination of the FCC's Third Report and Order and Third Further Notice of Proposed Rulemaking on CPNI (section 2.7, above) and its order declining to promulgate fair location information practices rules (section 2.8) can only leave the telecommunications industry uncertain about the requirements for consumer consent to use of location information. The Third Report and Order gives companies the choice of offering consumers either opt-in or opt-out consent to the use of location information by the primary company, its affiliates, and joint venture partners. This makes it seem as if one mechanism is as good as the other, without really answering the question of whether or not opt-in consent can ever be assumed. By declining to approve the CTIA position on fair location information practices, the FCC has refused to clarify the required mechanism for consumer consent to the use of location information. To the extent that the E911 legislation was specifically designed to apply to circuit-switched devices governed by an EUI-164 telephone number, its applicability to newer technologies, such as cellular Internet access and Wi-Fi (WLAN or 802.11) is unclear and perhaps not relevant depending on interpretation, though it might arguably be applied to Internet telephony where EUI-164 telephone numbers are still used.

2.10 Legislation in the 108th Congress

Two bills that would affect location privacy have been introduced in the current session of Congress. Both have been referred to committee and neither is expected to pass into law.

H.R. 71, titled "The Wireless Privacy Protection Act,"³⁷ would amend Section 222 of the Telecommunications Act of 1996 to require a customer's express prior authorization for the use of location or crash information, based on very explicit notice to the customer of the carrier's policies on collection and use of information.

HR 122, the "Wireless Telephone Spam Protection Act,"³⁸ would prohibit the sending of unsolicited commercial messages (text, graphics, and images) to cell phones.

Senator John Edwards's "Location Privacy Protection Act" would have required "express authorization," or opt-in consent, for the use of location information, but it died in committee in the 107th Congress,³⁹ and has not been reintroduced.

2.11 State Laws Concerning Wireless Location Information

The FCC's July 16, 2002, CPNI order (Third Report and Order and Third Further Notice of Proposed Rulemaking) does not pre-empt states from enacting their own rules for location information (see section 2.7). In November 2002, the Washington State Utilities and Transportation Commission (WUTC) enacted CPNI regulations that are entirely opt-in. In addition to requiring clear and effective notice of collection and use of CPNI, the rules protect call detail (date, time, duration, and number dialed) and limit information sharing only to commonly owned companies of the telecommunications carrier.⁴⁰

In California, the Public Utilities Commission (CPUC) has proposed a Telecommunications Consumer Bill of Rights with this generic-sounding privacy provision: "Consumers have a right to personal privacy, to have protection from unauthorized use of their records and personal information, and to reject intrusive communications and technology."⁴¹ It has not ruled yet on consent to use of CPNI, but presumably it will in the consumer protection rules to be promulgated under the Bill of Rights. Note that California has an anti-spam law passed in 2002 that bans sending unsolicited text messages to cell phones.

2.12 State DMCA Laws

The Digital Millennium Copyright Act (DMCA) is a 1998 law enacted to enforce copyright protection in the digital sphere. Implementation of the DMCA requires the means of controlling access to copyrighted material and also of monitoring access—known as digital rights management, or DRM. Cellular Internet access puts telephones in the category of devices that could be used to obtain copy-protected material. Recently, the Motion Picture Academy of America (MPAA), one of the prime enforcers of the DMCA, has been encouraging states to pass their own versions of the DMCA. To that end, the MPAA has written a model act for states to follow.⁴²

The DMCA intersects with the issue of wireless location privacy because, in order to control—and prosecute—unauthorized digital copying, it is necessary to know the identity and location of the person using the devices that does the copying. The model act proposes civil and criminal penalties for developers and users of devices, including cellular telephones, which conceal “the existence or place of origin or destination of any communication.”⁴³ Mostly likely in response to pressure from the telecommunications industry, the MPAA revised the model legislation to require *criminal* intent to conceal location for liability under the act, though the original did not have this provision.

Several states have enacted versions of this act, and legislation is pending in others. Arkansas makes concealment of location information illegal only if criminal intent is involved; South Carolina requires “fraudulent intent.” Some states have made concealment illegal regardless of intent, including Delaware, Illinois, Michigan, Pennsylvania, and Tennessee. Pending legislation in Texas makes it a crime to “conceal from a communication service provider, or from any lawful authority, the existence or place of origin or destination of any communication,” regardless of intent. The governor of Colorado vetoed a location concealment law in May 2003.⁴⁴

The difficulty with many of these acts is that, to the extent they omit criminal intent as a motivation for the concealment of location information, they could criminalize some commonly used technologies in today’s Internet. Many home users, enterprises, and some wireless ISPs commonly use Network Address Translation (NAT) technology to provide additional IPv4 addresses due to the perceived shortage of IPv4 address space. A side effect of this technology is that, from outside the NAT addressing realm, the actual location of the IP host within the private addressing realm is obscured, because the outside host only has an IP address for the NAT translation box at the topological border of the realm.

2.13 U.S. Conclusions

The FCC’s rulemaking on the Telecommunications Act of 1996 and the 1998 E911 amendments to the Act concerning CPNI and customer consent has had two consequences:

- (1) The Commission has left the industry uncertain as to whether the appropriate and legal consent mechanism required for the use of CPNI is opt-in or opt-out; and
- (2) By not pre-empting states from regulating in this area, the Commission has assured that states with a history of protecting consumer privacy (or that discover a need to protect consumer privacy because of the rising visibility of identity theft as a political issue) will enact stronger regulations. This leaves companies gearing up to offer location-based services and mobile commerce applications with no clear guidance about how to proceed, and the likelihood of having to comply with a patchwork of state notice and consent

requirements. The absence of legislative and administrative clarity on an issue that has real popular resonance because of its implications for stalking, identity theft, and spam, is bound to encourage regular efforts to “fix” the problem with further legislation at both the state and federal levels.

The appearance of the DMCA in state legislatures, with the encouragement of the crusading Motion Picture Association of American, should also be watched. It seems unlikely that efforts to prevent concealment of a cellular customer’s location to deter theft of service could be interpreted as a bar on allowing customers to opt-out of the use of their location information. Use of the DMCA to prevent copyright violations that may occur by means of cellular Internet access, however, is a very real possibility.⁴⁵ In addition, many of the state efforts, through lack of careful attention to delineation between criminal and noncriminal intent, may have the effect of outlawing what are today commonly used technologies for increasing Internet access. This problem – lack of clear delineation of intent – has plagued DMCA since its inception.

In an environment of regulatory confusion and overlapping regulatory initiatives emanating from a public policy perspective that is beginning to look very anti-competitive (the copyright enforcement impetus), companies are likely to err on the side of caution. Public reaction can be harsh and swift in cases of perceived misuse of information by Internet companies, as shown by the example of DoubleClick’s online information collection practice of combining web surfing profiles with personally identifying information, in violation of its own privacy policy.⁴⁶

Misuse of location information is a highly sensitive issue, and as far as location-based services and mobile commerce are concerned, if consumers doubt the privacy and security of any service, its viability will be threatened. Since the Federal Communications Commission appears to lack the will (or the political makeup) to untangle the regulatory knots it has tied around consumer consent to the use of CPNI, it is in the interest of the telecommunications industry to adopt and actively promote practices that will encourage consumer trust through a clear notice of what the policies on collection and use of CPNI are, and a clear and meaningful opportunity either to opt in or opt out. The industry should consider as a prototype the model Fair Location Information Practices proposed by the Cellular Communications and Internet Association (CTIA) in its rulemaking request to the FCC (see section 2.8, above). These would assure consumers of clear notice of a company’s policy regarding the collection and use of location information and would establish their express authorization (opt-in consent) as the standard for use of that information.

The U.S. telecommunications industry should also look to Japan’s treatment of consumer consent as the foundation for the Japanese telecommunications industry’s successful marketing of location-based services. In 1998, the Japanese Ministry of Posts and Telecommunications set a clear standard for consent to use of location information: “A telecommunications carrier shall not disclose the location information (the information indicating the location of the party in possession of a mobile terminal) to another except when the data subject gives consent . . .”⁴⁷

This unambiguous consent requirement has enabled location-based cellular services to take off in Japan, to the great convenience of the public, which can use these services without the fear of being tracked or the annoyance of being targeted. To take one example, DoCoMo’s “Imadoko” (“where am I now?”) service provides very precise location information that can be used to monitor the location of small children or aged parents. The service contract permits the release of the information only to specified people, usually family members, and this information is unavailable to others. American consumers would no doubt be willing to pay for similar services and would find a similar consent mechanism both reassuring and unobtrusive. Nothing in the FCC’s consent rulings to date prevents the utilization of a similar scheme in the United States.

SECTION 2: WIRELESS LOCATION PRIVACY IN THE EUROPEAN UNION

In this section, we discuss the development of data protection laws in the European Union and then consider the Directive on Privacy and Electronic Communications and its implementation by member states. Two parts of the Directive are highlighted: regulation of location data and data retention requirements.

3 Introduction: Data Protection in the European Union

The history of data protection in the European Union is far more coherent and uniform than it is in the United States. The perceived need for data protection in European countries is founded on the strong social belief that personal data is private and should be protected against government abuse. Early implementation of protective laws prevented personal information from becoming a commodity, as it is in the United States, where only certain types of data have statutory protection that regulates or limits its use by private business.

3.1 Organization for Economic Cooperation and Development Data Protection Guidelines

The European Community recognized data protection as a public policy issue as early as 1980, when the Organization for Economic Cooperation and Development (OECD) issued a set of guidelines for protection of personal data.⁴⁸ In summary, the OECD guidelines propose limited collection of personal data. They call for accuracy; notice; use for a specific purpose, with the data subject's consent required for any other use; security; individual access, with the right to challenge, correct, and expunge one's personal files; and for data collectors to be held accountable for compliance with regulations. The Community has consistently carried these privacy principles forward as it has codified its rules for governance.

3.2 The 1995 Data Protection Privacy Directive

The principle European Union (EU) document on information privacy is the 1995 Data Protection Directive.⁴⁹ This codifies protection of personal information and requires the Community's member states to harmonize their privacy laws in accordance with it. The Directive, which has now been enacted throughout the EU (and also by many EU trading partners), sets a high standard of privacy protection and ensures that privacy is on member governments' policy-making agendas. Not only must EU states pass laws that protect personal information in both the private and public sectors, but also these laws must provide for blocking the transfer of information to non-member states that do not provide an "adequate" level of protection.

The Directive establishes "fair information practices" similar to those promulgated in the OECD guidelines as the basis for all processing of personal data.⁵⁰ Articles 6 and 7 concern the proper legal basis for data processing. In general, no data can be processed that is not contractually or legally necessary without the informed and unambiguous consent of its subject. Data may not be used for any purpose other than the one for which it was collected without consent. Data subjects have the right to access their data, the right to know its source whenever possible, and the right to correct errors. Subjects must be notified of the purpose of data processing, who will receive their data, and whether or not giving their data is obligatory; they may opt out of its use when that is possible. Subjects also have a right of action for unlawful use of their data.

It is important to note that the EU enforces its data protection policies beyond its borders.⁵¹ In early 2002, the European Commission released the final form of data privacy contractual clauses

for the transfer of personal data for processing outside the EU.⁵² Exceptions to the standard are allowed for countries and companies that adhere to Safe Harbor principles.⁵³ With regard to location information, there are exceptions for transfer of personal data outside the EU if the data subject consents or has a contractual agreement with the data controller. Also, companies may rely on contracts approved at the national level by member states' data protection commissioners.⁵⁴

3.3 The 1997 Telecommunications Privacy Directive

The Telecommunications Privacy Directive was approved by the EC in 1997.⁵⁵ It supplements the 1995 Data Protection Directive by making specific provisions for telecommunications services, including telephones, digital TV, mobile networks, and the Internet. It obligates carriers and service providers to ensure the privacy of users' communications, and in particular, it requires that "traffic data" be erased when the billing cycle is completed.⁵⁶ Although the directive applies to "public digital mobile networks,"⁵⁷ its definition of traffic data does not expressly include location information.

3.4 The 2002 Directive on Privacy and Electronic Communications

In July 2002, the European Commission passed the Directive on Privacy and Electronic Communications to reflect continuing technological developments in the communications sector.⁵⁸ This in effect replaces the 1997 Telecommunications Directive, establishing "technology-neutral" legal standards for privacy protection in the processing of personal data for all electronic communications. It is part of a larger package of five related directives intended to strengthen competition within European markets.⁵⁹

3.4.1 Location Information, or Localization

Article 9 of the Privacy and Electronic Communications Directive expressly recognizes and regulates the use of cellular location information. A recital that precedes the articles of the Directive distinguishes location data from other types of traffic data:

In digital mobile network, location data giving the geographic position of the terminal equipment of the mobile user are processed to enable the transmission of communications. Such data are traffic data covered by Article 6 of this Directive. However, in addition, digital mobile networks may have the capacity to process location data which are more precise than is necessary for the transmission of communications and which are used for the provision of value added services such as services providing individualised traffic information and guidance to drivers. The processing of such data for value added services should only be allowed where subscribers have given their consent. Even in cases where subscribers have given their consent, they should have a simple means temporarily deny processing of location information, free of charge.⁶⁰

Article 9 requires location information to be processed anonymously unless it is being used with the subscriber's consent to provide a value-added service. To obtain consent, the service provider or data collector must inform subscribers what kind of location data will be used, for what purpose and for how long, and whether the data will be transmitted to a third party for the purpose of providing a service. The unambiguous meaning of Article 9 is that informed opt-in

consent is required for the provision of location-based services. In addition, consent is not open-ended: subscribers must be able, without charge, to withdraw their consent for the collection or processing of their location information at any time.⁶¹ Article 9 leaves it to member countries to decide what constitutes consent and how it is to be obtained and withdrawn.

3.4.2 Data Retention

A major issue in the debates over the Directive on Privacy and Electronic Communications, because they followed the terrorist attacks in the U.S., was whether governments could compel communications service providers to retain traffic data (that is, transactional information, not content) for national security or law enforcement purposes. As a general rule under the Directive, traffic data collected for billing purposes must either be erased or made anonymous when it is no longer needed (that is, when the billing cycle is completed).⁶² Ultimately, over the strong objections of civil rights groups, telecommunications companies, and ISPs,⁶³ data retention provisions were included that permit—but do not require—telecommunications operators and Internet service providers to record, index, and store their subscribers' data for all communications over cellular and land line phones, via fax and email, in chat rooms, on the Internet, or on any other electronic communication device.⁶⁴ Both traffic and location information may be retained.

The practical effect of the 2002 Directive's data retention policy is to reverse the 1997 Telecommunications Privacy Directive, which requires that traffic data be erased after it is no longer needed to complete a communication or for billing purposes.⁶⁵ It is up to individual member states to pass data retention laws, although the inclusion of this provision in the Directive is seen by many as encouragement to do so. Thus far, the UK, France, Belgium, and Spain have enacted such laws; Ireland issued a Directive in April 2002 that requires traffic data to be available to law enforcement for three years.⁶⁶ Finland's draft law omits data retention. It appears that the remaining EU members, with the exception of Germany and Austria, will all eventually pass such laws.⁶⁷

3.5 Implementation of the Directive on Privacy and Electronic Communications

EU member countries have until October 31, 2003, to implement the Directive on Privacy and Electronic Communications. Most have not yet done so and many will not have completed the process by the October deadline. However, as conceived by the EC, the Directive appears to leave little room for national variations.⁶⁸ This has to do with the underlying reason for passage of the entire package of electronic communications directives: to promote the development of a coherent and competitive European telecommunications market. To help accomplish this goal, the new regulatory framework for electronic communications establishes the European Regulators Group (ERG) for electronic communications networks and services, to act as the interface between the regulatory authorities for telecommunications in member states and the European Commission, to ensure consistent application of the framework.⁶⁹

3.6 Status of Implementation of the Directive in EU Member Countries

The table that follows summarizes EU member states' implementation of the Directive on Privacy and Electronic Communication (2002/58/EC) to date. It highlights treatment of Article 9, the section that deals with mobile location information. It includes information on Article 15, data retention, where that is available.

COUNTRY	SUMMARY OF REGULATIONS	REFERENCES
AUSTRIA	Austria has not yet implemented directive 2002/58/EC. The federal Ministry of Transportation, Innovation and Technology (BMVIT) has drafted a new communications (Kommunikationsgesetz) act (not yet published) to implement the directive. The draft is expected to be introduced in parliament in the near future. Currently, telecommunications data protection and privacy is governed by chapter 12, sec 87-101 of the Telecommunications Act of 1997, Bundesgesetzblatt (federal law gazette) I Nr 100/1997 as amended by BGBl I Nr 134/2002. ⁷⁰	Amended Telecommunications Act of 1997 (in German): http://www.rtr.at/web.nsf/deutsch/Telekommunikation~Regulierung~Rechtsinfos~Rechtsinformationen~TKG Ministry of Transportation, Innovation and Technology: http://www.bmvit.gv.at
BELGIUM	Belgium has so far implemented only Article 13 of 2002/58/EC, the provision on unsolicited commercial communications. No drafts for the other provisions have been written yet. ⁷¹ An earlier Computer Crime Act requires compulsory data retention for one year.	Institut Belges des service postaux et des telecommunications (in English): http://www.ibpt.be/bipt_E.htm
DENMARK	The Executive Order on the Provision of Telecommunications Networks and Telecommunications Services implementing 2002/58/EC came into effect on July 25, 2003. Regulation of the use of mobile location data conforms to Article 9 of 2002/58/EC. Data retention for law enforcement purposes is required. ⁷²	National IT and Telecom Agency of Denmark (in English): http://www.itst.dk/mainpage.asp Note that the law will be posted on the agency's web site in English at around the time it takes effect.
FINLAND	The Framework Directive of 2002/58/EC was implemented on July 27, 2003. A draft proposal of the Act on Privacy and Electronic Communications is expected to be submitted to Parliament in September 2003. The draft Act requires subscribers' consent to use of location data; data retention is not included in the draft. The Act is currently undergoing official translation. ⁷³	A summary of the Communications Market Act (but not the Privacy and Electronic Communications Directive), introduced May 5, 2003, by Ministry of Transport and Communications is available (in English): http://www.mintc.fi/www/sivut/english/tele/communicationspolicy/index.html
FRANCE	France is in the process of drafting a law to implement 2002/58/EC. The law will follow Article 9 of the Privacy and Electronic Communications Directive in requiring mobile subscribers' informed consent to use of location data, except in emergency situations. France has already implemented Article 15, the data retention provision of the Directive. ⁷⁴	Information concerning telecommunications legislation (in French): http://www.telecom.gouv.fr/

COUNTRY	SUMMARY OF REGULATIONS	REFERENCES
GERMANY	A draft law implementing 2002/58/EC is currently in the comment period. The section which regulates mobile location information is similar to that in Article 9 of the EC directive. Germany did not implement data retention. The law is expected to come into effect in late 2003 or early 2004. ⁷⁵	Regulatory Authority for Telecommunications and Posts (in English): http://www.regtp.de/en/index.html Bundesbeauftragten für den Datenschutz (BfD) (in English): http://www.bfd.bund.de/information/engl_corner.html Draft law for electronic communications (in German): http://www.eadp.be/main7/position/german%20draft.pdf
GREECE	Deadline for public comment on draft legislation to implement the package of electronic communications directives, including 2002/58/EC, was July 4, 2003. Greece has implemented the earlier Directive on Privacy in Telecommunications, which remains in effect until the more recent directives have been transposed.	National Telecommunications and Posts Commission (in English): http://www.eett.gr/eng_pages/index2.htm
IRELAND	The electronic communications directives, including the privacy directive (2002/58/EC), have not been implemented yet. An April 2002 Directive requires retention of traffic data for three years for law enforcement purposes. Comments on other aspects of the directives than privacy may be found at the first web site listed in the next column. ⁷⁶	Commission for Communications Regulations: http://www.odtr.ie/docs/ComReg0312.doc Department of Communications, Marine and Natural Resources: http://www.dcmnr.gov.ie/display.asp/pg=929 (Electronic Communications Regulatory Package)
ITALY	No information on the implementation of 2002/58/EC is currently available.	
LUXEMBOURG	No information on the implementation of 2002/58/EC is currently available.	
NETHERLANDS	A draft of the Telecommunications Act (TA) which implements 2002/58/EC has already been sent to Parliament. It is expected to be enacted into law before November 1, 2003. The TA section concerning mobile location data (Article 11.5a) is similar to Article 9 of 2002/58/EC. With regard to data retention, the TA states that the traffic data shall not be retained for a longer period of time than is necessary to complete a bill-paying cycle; a data retention exception for purposes of criminal investigations is still under discussion (Article 11.5). ⁷⁷	Ministry of Economic Affairs (English option available): http://www.ez.nl/default.asp

COUNTRY	SUMMARY OF REGULATIONS	REFERENCES
PORTUGAL	The new basic law to transpose all five electronic communications directives, including 2002/58/EC, is still in draft form; it is not known when it will be implemented. ⁷⁸	National Communications Authority (ANACOM) (in English): http://www.anacom.pt/index.jsp?categoryId=2958
SPAIN	<p>A new General Law for Telecommunications to implement all the EC telecom directives, including the Directive on Privacy and Electronic Communications, was approved by the Council of Ministers on March 7, 2003. The law, amended by the Senate's Commission on Science and Technology, will be resubmitted to the Congress. Approval is required, but it is not known now when the law will be voted on.⁷⁹</p> <p>Spain's "Law of Information Society and Electronic Commerce" (Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, or LSSI) came into effect in October 2002. The law principally concerns Web-based commerce, but its 1-year data retention requirement includes mobile location information, which must be securely stored by telecom companies.⁸⁰</p>	Law of Information Society and Electronic Commerce (in Spanish): http://www.setsi.mcyt.es/legisla/internet/ley34_02/sumario.htm .
SWEDEN	<p>The Swedish Parliament recently adopted an Act on electronic communications ("Lag om elektronisk kommunikation") which implements 2002/58/EC, including Article 9. This legislation took effect on July 26, 2003. The law states that localization data may be processed only if it has been anonymized or if the user or subscriber has given his/her consent to the processing.⁸¹</p> <p>Note that It is unclear at this time whether Sweden has implemented Article 15, requiring data retention.</p>	<p>Legal text will be posted in Swedish sometime in July 2003: www.lagrummet.se.</p> <p>National Post and Telecomm Agency (in English): http://www.pts.se/Default.asp?SectionID=&ItemID=&LanguageID=EN.</p>
UK	<p>The UK draft implementing Article 9 of 2002/58/EC states, "[it is] important that subscribers and users give their informed consent and understand the data processing implications of this kind of service. . . [but does] not propose to specify exactly how service providers should go about this in the Regulations."⁸²</p> <p>The comment period for the draft proposals ended on June 19, 2003, and it seems possible that the UK may meet the October implementation deadline</p>	Department of Trade and Industry: http://www.dti.gov.uk .

3.7 EU Conclusions

Eventually, the Directive on Privacy and Electronic Communications will be fully implemented throughout the EU, although this almost certainly will not happen by the October 31, 2003, deadline. The clear intention of the European Council in passing the package of directives (of which 2002/58/EC is one) is to stimulate competition in the electronic communications market. With some exceptions (such as Article 15 on data retention), the privacy directive leaves little room for national variations, so it should be assumed that regulations concerning mobile location information will conform to Article 9. That is, location data must remain anonymous except when used with a subscriber's informed consent, to provide "value-added services." It may be used only for the service consented to and subscribers must be able to withdraw their consent at any time. In countries that implement the data retention provision of the Directive (Article 15), telecommunications providers will be required to retain traffic data, including location data, securely and for whatever period is specified. Finally, companies that wish to provide location services from outside the EU must comply with the 1995 Data Protection Directive or with Safe Harbor principles.

SECTION 3: WIRELESS LOCATION PRIVACY IN JAPAN

In this section, we discuss the development of data protection laws in Japan. The analysis includes a discussion of the interrelationship between the new Personal Data Protection Law and the 1998 "Guidelines on the Protection of Personal Data in Telecommunications Business" that regulate the use of wireless location information.

4 Introduction: Privacy Law in Japan

Japan has a constitutional history of protecting privacy. More recent legislation has recognized the need to protect the privacy of electronic data, motivated in part by the business necessity of compliance with EU data protection directives. The "Guidelines on the Protection of Personal Data in Telecommunications Business" gave the telecommunications industry clear rules to follow for use of location information in 1998, which is no doubt a significant factor in Japan's pre-eminence in the location-based services market.

4.1 Constitutional Privacy

Article 21 of Japan's 1946 Constitution states that "the secrecy of any means of communication [shall not] be violated." While this clause could not have anticipated mobile telephones and wireless communication, there is no reason to believe it does not apply to them. In addition, Article 35 of the Constitution grants "The right of all persons to be secure in their homes, papers and effects against entries, searches and seizures shall not be impaired except upon warrant issued for adequate cause. . ." ⁸³ Both articles provide important precedents for the protection of individual privacy in Japanese law, and they have been carried forward in the statutory law as it has evolved.

4.2 Protection of Computerized Personal Data Held by the Government

The 1988 Act for the Protection of Computer Processed Personal Data Held by Administrative Organs protects Japanese citizens from government misuse of computerized personal information. ⁸⁴ This law, which is modeled on the 1980 OECD guidelines for personal data protection, covers all computerized data held in the public sector. ⁸⁵ With exceptions for national security and law enforcement, citizens are entitled to notice of what is in their file, who controls it, the purpose for which the data is collected, and how it is collected. Data subjects must have

notice of whether or not third parties will have access to their information; third-party dissemination should be strictly limited in any case. Individuals may request in writing to see their information and correct it. The government must take reasonable precautions to keep computerized data secure. In addition to the national legislation, around a third of the local governments in the country have enacted their own, often stricter, laws to protect the privacy of computerized personal information.

4.3 The Personal Data Protection Law

On May 23, 2003, the Diet passed a final version of a package of Personal Data Protection bills that were first introduced in 2001, bringing Japan more closely in line with the European Union on privacy protection.⁸⁶ The new law recognizes the society's ever-increasing reliance on advanced electronic communications technology, which the government strongly endorsed in the 2000 Basic Law on the Formation of and Advanced Information and Telecommunications Network Society in 2000.⁸⁷ The Basic Law promotes the expansion of e-government, online education, and identifies the Internet as a basis for improving the life of the society in general.

The new Data Protection Law recognizes the need in an Internet-based society to secure the immense volumes of personal information it collects and generates against misuse and leaks. The legislation consists of five bills. Three of the five impose tighter restrictions on the way that private companies, public administrators, and independent organizations (such as nonprofit or non-governmental organizations) handle personal information; the remaining two call for the establishment of a council to handle complaints concerning abuse of personal information and for working out related privacy bills as needed to complement the underlying legislation (such as laws to regulate financial and medical information).⁸⁸

In order to overcome vociferous objections from media and opposition parties that the laws presented a threat to freedom of the press and freedom of speech, the government omitted a section of so-called "basic rules," which would, among other things, have established procedures to follow for acquisition of private data that required participation of individuals whose data was being acquired. The rules would also have mandated accuracy, security, and transparency in the use of data, a burden that almost all media organizations believed would have severely inhibited their ability to report the news. The basic rules would have applied to all entities, government and private, that handle personal information. As passed, however, the law exempts media organizations, freelance writers, academic organizations, religious organizations, and political institutions.⁸⁹

4.4 How the Personal Data Protection Law Affects the Business Sector

One of the bills passed as part of the Personal Data Protection Law specifically regulates how businesses may collect and use personal information:

- Businesses must notify individuals that their personal information is being collected and of the purpose for which it is being used; information may be used only for the stated purpose.
- Businesses that collect personal information must obtain the subject's consent before passing information on to third parties.
- Individuals have the right to see and correct personal data, and to withdraw consent to its use.
- Businesses are required to take reasonable measures to keep personal data secure.

- Individuals may complain to the relevant ministry (for example, the Ministry of Posts and Telecommunications) about misuse of their personal information and the minister will enforce the law and may impose penalties.

It is clear from the range and complexity of the overall legislation that a great deal more law-making will be needed to establish procedures and structures for carrying out the new law. Observers have also noted that the government should be responsible for educating the public and the regulated sectors about how the bill works and the steps they need to take to be in compliance with it. The government is expected to create an agency to handle complaints and also to write specific laws or regulations that apply to telecommunications, financial, and medical information. The obligations of businesses that handle personal data will go into effect in two years; it is not now known when penalties for misuse of data will take effect.⁹⁰

4.4.1 The Personal Data Protection Law and Wireless Location Information

The Personal Data Protection Law does not specifically regulate wireless location information, but it does cover “carriers which use personal data for their operational purposes.”⁹¹ This language would appear to cover only traffic data. Since the Ministry of Posts and Telecommunications’ “Guidelines on the Protection of Personal Data in Telecommunications Business” (see section 4.5 below) already specifically define and regulate location information, however, it is likely that further legislation applying the provisions of the Personal Data Protection Law to the telecommunications sector will be based on these Guidelines.

4.5 Guidelines on the Protection of Personal Data in Telecommunications Business

The Ministry of Posts and Telecommunications issued “Guidelines on the Protection of Personal Data in Telecommunications Business” in 1998.⁹² The Guidelines were written in recognition of the need to “improve the convenience of telecommunications services” and to protect telecom users’ privacy rights from “infringements of personal data along with the increases in its distribution in the high-tech info-communications-based social environment, accompanied by the public nature of telecommunications services.”⁹³ The Guidelines are not binding, but they provide an official standard for data practices and they have been followed by businesses developing location-based services and mobile commerce applications. As noted above, it seems certain that the Guidelines will be the basis of further legislation that specifically regulates handling of personal information by the telecommunications industry under the Personal Data Protection Law.

Article 6 of the Guidelines protects traffic data (the information needed for connection and billing, which does *not* include content) from disclosure without consent.⁹⁴ Article 11 designates location information as a separate category of personal information. It unambiguously states that a “telecommunications carrier shall not disclose the location information (the information indicating the location of the party in possession of a mobile terminal) to another except when the data subject gives consent.” For disclosure without consent, there must be a warrant issued by a judge, an on-going criminal investigation, a life-threatening emergency, or “some other legal ground for exception.”⁹⁵

The relatively early publication of these Guidelines made it clear to the telecommunications industry, providers of location-based services, and any business interested in developing mobile commerce, what was required regarding use of subscriber data. This has been one important factor in encouraging the rapid expansion of mobile commerce in Japan, just as the absence of regulatory clarity in the U.S. and the belated issuance of the 2002 Directive on Privacy and

Electronic Communications (repealing the 1997 Directive on Telecommunications) in the EU have somewhat hindered its development in the countries concerned.

4.6 Japan Conclusions

Japanese society is in the process of being transformed by wireless communications, and it is no exaggeration to describe this transition as revolutionary in its effect on the ways that people communicate and access information. Continued progress is assured, now that the government is working to remove the structural and regulatory blocks that restricted telecommunications and Internet development in the 1990s. Its recent legal and regulatory guidance has been timely and practical, encouraging competition and lowering costs, particularly in the mobile communications field.

The 2000 Basic Law on the Formation of an Advanced Information and Telecommunications Network Society, as its name clearly states, is a strong declaration of a national industrial and social policy with the goal of making Japan an advanced networked society, for the benefit of all citizens.⁹⁶ Even prior to passage of the Basic Law, mobile telecommunications and commerce were already quickly becoming an indispensable part of peoples' daily—or, more accurately, minute-by-minute—lives in Japan. With a population of 127,000,000, more than half of all Japanese already have 3G telephones. Only four years after the introduction of mobile Internet service in 1999, more than half the population subscribes.⁹⁷

The significance of protecting mobile subscribers' traffic and location data as the mobile industry grows cannot be underestimated. The Ministry of Posts and Telecommunications 1998 Guidelines opened the way for business development and consumer security by clearly requiring consent for the use of location information. Now the new Personal Data Protection Laws, once they are fully implemented, will create an administrative and enforcement structure to ensure that individuals are informed about any collection their personal data and have the ability to consent to its use.

5 General Conclusions

Right now is a very exciting time in the wireless communications industry. New wireless devices have come a great distance from the simple mobile telephones and personal desk assistants they were originally. With new hardware and vastly increased transmission capabilities formerly separate functions of phones and PDAs overlap and new ones, such as the ability to take and transmit still photos and videos, as well as display them locally, have been added. Bring wireless Internet access to the mix and what you have in your hand is no longer a phone or a digital calendar/address book, but an almost weightless portable computer.

Laws and regulations, which play a significant role in business development by providing an industry with guidance about what it may or may not do, struggle to keep up with the issues that rapidly changing technologies present. Law, encumbered by multiple Byzantine processes, is inherently slow-moving and, where it encounters technology, is almost always reactive. Law and rule-making bodies around the world are now embarked on a process of attempting to control at least some of the privacy protection challenges posed by wireless communications technology. In doing so, they must balance a generally recognized need to prevent abuse of personal data against the need to keep data flowing in economies and societies that increasingly consume and depend on ever-growing quantities and varieties of it.

Of the countries covered by this paper, some governments have been more successful than others

in accomplishing data protection and giving guidance to industry. In the case of the United States regulations governing the use of wireless location information are ambiguous, making it difficult for a business that wants to offer location-based services to know what is required to obtain a subscriber's consent to the use of location information. As the Federal Communications Commission, the rule-making authority for the telecommunications industry, has left it, telecommunications companies may choose either opt-in or opt-out consent. This makes it unclear whether, in signing up for a service, consumers automatically give their consent and should be offered a chance to opt out, or if they should be asked to opt in to the use of their information at the time they subscribe to a service. Since the choices seem to contradict each other, it is impossible for a business to proceed with a clear assumption that it has regulatory backing, whatever it does.

Another impediment to the growth of location services is that, currently, states are not pre-empted from enacting their own regulations for consent to use of location information. Washington State has already done this and California has a pending Telecommunications Consumer Bill of Rights that may establish opt-in consent requirements. The fact that location-based services may be regulated very differently from state to state hinders the growth of a national model for offering such services.

Individual state versions of the Digital Millennium Copyright Act (DMCA) represent another threat to the wireless industry and location services, because they would criminalize manufacturing, selling, or using any device or application that conceals location. Several states have already passed such laws.

Finally, the development of a wireless location infrastructure to implement the Wireless Communications and Public Safety Act (WCPSA) is proceeding exceptionally slowly. Telecommunications companies have repeatedly asked for extensions on the implementation deadline, which has been pushed back to 2005. Hardware manufacturers are slowly implementing the FBI's demand to build surveillance features (i.e., wiretapping capability) into cellular handsets, based on the Communications Act for Law Enforcement (CALEA).

All of these factors lend their own uncertainties to the future of wireless location services in the United States. Europe, however, should have a clear regulatory framework for electronic communications in place within the foreseeable future. The EU's fifteen member states can be expected to adopt the location information consent section of Directive on Privacy and Electronic Communications that provides clear guidelines for the use of this information, if not on how consent should be given or withdrawn. While nine of the fifteen member states are likely to pass laws on data retention, including location data, it is difficult to predict how this will affect acceptance of location-based services.

The European-standard Wireless Application Protocol is generally acknowledged to be slower than acceptable for anything more than primitive wireless Internet use, but it should be swept away by 3G capability. Based on the arrival of regulatory clarity in Europe, EU member countries should be ready for considerable growth in location-based services.

Japan is still the location services leader, in both regulations and technology. Although implementation of the new Personal Data Protection Law and its application to the telecommunications industry may be an arduous and lengthy process, there is no reason to expect it to impinge on the on-going, highly effective role of the "Guidelines on the Protection of Personal Data in Telecommunications Business," which have already played a part in giving Japan its considerable head start in location-based services. The location enterprise is already

firmly rooted, and the seemingly inexhaustible trendiness of new uses for mobile telephones should see to the continuing growth of location services.

Notes

¹ For more information on RFID tags and their potential as human tracking devices, see <http://www.nocards.org/AutoID/overview.shtml>.

² See the Cellular Telecommunications and Internet Association's web site wireless subscriber counter, updated daily: <http://www.wow-com.com/>.

³ "AT&T Wireless Helps Callers Find Friends," PCWeek, 6/26/02; <http://www.pcworld.com/news/article/0,aid,102269,00.asp> (general packet radio system—GPRS).

⁴ The FBI's demand that the telecommunications industry build surveillance features into cellular handsets, based on the Communications Act for Law Enforcement (CALEA), is slowly being implemented by hardware manufacturers. The USA Patriot Act substantially lowers the requirements for a warrant to tap a phone (it must relate only to a "significant purpose" of an investigation of alleged terrorism, and it is issued by FISA, a secret court) and applies the warrant to the user, not the means of communication, thereby covering any fixed or mobile phone used, as well as any Internet-enabled communications device.

⁵ Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 213 (1890).

⁶ *U.S. v. Miller*, 435 U.S. 425 (1976). The Supreme Court found no reasonable expectation of Fourth Amendment privacy protection against search and seizure in checks and deposit slips voluntarily conveyed to a bank in the ordinary course of business. The same reasoning has been applied to data voluntarily conveyed in the ordinary course of business, regardless of the entirely unrelated purposes—such as profiling by data miners—for which it may ultimately be used.

⁷ The IETF's "Geopriv Requirements" study offers an important analysis of location information security. The goal of the study is to propose standards and rules for protecting location information. The study strongly favors giving wireless users control of their own location information. The most current iteration (March 2003) of "Geopriv Requirements," by Jorge Cuellar, John B. Morris, Jr. (Center for Democracy and Technology), Deirdre Mulligan (Samuelson Law, Technology, and Public Privacy Clinic), Jon Peterson (NeuStar), James Polk (Cisco), can be found at <http://www.ietf.org/internet-drafts/draft-ietf-geopriv-reqs-03.txt>.

⁸ See 47 U.S.C. 222(h)(1): "The term 'customer proprietary network information' means (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship." Note: Section 222(f) was moved to Section 222(h) when the WCPSA was passed in 1999, amending the Telecommunications Act of 1996.

⁹ 47 U.S.C. 222(c)(1).

¹⁰ 47 U.S.C. 222(c)(3) permits the use of CPNI in the aggregate or collective form, from which all personally identifying information has been removed.

¹¹ Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, CC Docket No. 96-115, FCC 98-27; Final Rule; released Feb. 26, 1998; Sec. 64.2007(a): Notice and approval required for use of customer proprietary network information, 63 Federal Register 79, p. 20339.

¹² *Id.* at Sec. 64.2007(b).

¹³ *Id.* at Sec. 64.2007(f).

¹⁴ *Id.* at ¶¶ 39-41, pp. 20329-20330.

¹⁵ Id. at ¶ 2, p. 20327.

¹⁶ Id. at ¶ 22, p. 20328.

¹⁷ *U.S. West v. FCC*, 182 F.3d 1224 (10th Cir.1999); (cert. denied, 530 U.S. 1213, June 5, 2000).

¹⁸ Id. at 1238.

¹⁹ The *U.S. West* ruling, left standing when the Supreme Court denied certiorari, is a controversial one. It holds that CPNI—consumer’s personal information—is “commercial speech,” protected by the First Amendment. It also appears to limit the ability of Congress to give individuals the right to control their personal information, by setting a very high standard for restricting dissemination of that information: “In the context of a speech restriction imposed to protect privacy by keeping certain information confidential, *the government must show that the dissemination of the information desired to be kept private would inflict specific and significant harm on individuals, such as undue embarrassment or ridicule, intimidation or harassment, or misappropriation of sensitive personal information for the purposes of assuming another’s identity.*” (emphasis added) Id. at 1235; in other words, use of CPNI must amount to the tort of defamation or the crime of identity theft for Congress to protect it.

²⁰ 47 U.S.C. 251(e).

²¹ 47 U.S.C. 222(d)(4)(A).

²² 47 U.S.C. 222(f)(1).

²³ Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information, CC Docket No. 96-115; FCC 01-247; Clarification Order and Second Notice Further Notice of Proposed Rulemaking; February 19, 1998; ¶ 7 (CPNI Clarification Order); http://www.fcc.gov/Bureaus/Common_Carrier/Orders/1998/fcc98027.txt.

²⁴ 47 C.F.R. § 64.2007(c): “A telecommunications carrier relying on oral approval must bear the burden of demonstrating that such approval has been given in compliance with the Commission’s rules in this part.”

²⁵ CPNI Clarification Order, ¶ 7.

²⁶ Id. at ¶ 8.

²⁷ According to 47 C.F.R. § 64.2007(f).

²⁸ CPNI Clarification Order, ¶¶ 9-10.

²⁹ FCC Adopts Rules Resolving How Phone Companies Share and Market Customer Information,” FCC News, 7/16/02, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-224366A1.doc; note that the further proposed rulemaking referred to here solicits comments for rules governing what happens to consumer information held by companies that go bankrupt.

³⁰ Id. at p. 1.

³¹ Implementation of the Telecommunications Act of 1996; Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information (etc.), CC Docket No. 96-115, FCC 02-214; June 23, 1998; ¶ 18, p. 9; http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-214A1.pdf.

³² Petition of the Cellular Telecommunications Industry Association for a Rulemaking to Establish Fair Location Information Practices; <http://www.cdt.org/privacy/issues/location/001122ctia.pdf>.

³³ Id. at pp. 10-11; it also requests safe harbor for any company that subscribes to these principles, at p. 2.

³⁴ In the Matter of the Request by the Cellular Telecommunications and Internet Association to Commence Rulemaking to Establish Fair Information Practices, WT Docket No. 01-72, FCC 02-208; July 24, 2002; http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-208A1.doc

³⁵ 47 U.S.C. § 222(f); WCPSA (E911) amendment to the Telecommunications Act of 1996.

³⁶ Id. at pp.3-4.

³⁷ HR 71, 108th Congress; <http://thomas.loc.gov>.

³⁸ HR 122, 108th Congress; <http://thomas.loc.gov>.

³⁹ S 1164, 107th Congress: <http://thomas.loc.gov>.

⁴⁰ “Washington regulators adopt nation’s strongest telephone customer-privacy rules,” Nov. 7, 2002:

<http://www.wutc.wa.gov/webdocs.nsf/6f0baa33f074e151882566c20000604d/93d4130392518ad988256c6a0060f5a5>

⁴¹ California Public Utilities Commission, “Telecommunications Consumer Bill of Rights” (draft); <http://www.cpuc.ca.gov/static/Industry/Telco/billofrights.htm>.

⁴² The MPAA’S “Draft Model Communications Security Legislation” can be found on Professor Edward Felten’s web site: http://www.freedom-to-tinker.com/doc/2003/mpaa_3apr.rtf.

⁴³ Id. at p. 2.

⁴⁴ Links to state DMCA laws can also be found on Prof. Felten’s Freedom to Tinker web site at <http://www.freedom-to-tinker.com/superdmca.html>.

⁴⁵ Now that a U.S. District Court has given the Recording Industry Association of America (RIAA, the other principal enforcer of the DMCA) the authority to obtain the names of individuals who use file-sharing to download music from the Internet, the RIAA is proceeding with individual lawsuits against what it considers copyright abusers. See Paul Roberts, “RIAA takes aim at individual swappers; Group will seek subscriber info from ISPs,” IDG News Service, 6/25/03; http://www.infoworld.com/article/03/06/25/HNriaaim_1.html?networking.

⁴⁶ In February 2000, the Electronic Privacy Information Center (EPIC) filed a complaint with the FTC asking the Commission to enjoin DoubleClick from its online profiling practices and alleging that the company had violated its own privacy policy (http://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf). The FTC investigated and found that DoubleClick had not violated its privacy policy, but the company was the target of a great deal of negative publicity during the year-long FTC investigation.

⁴⁷ “Guidelines on the Protection of Personal Data in Telecommunications Business,” Ministry of Posts and Telecommunications, Japanese Government December 2, 1998; Article 11, no. 1; http://www.soumu.go.jp/joho_tsusin/whatsnew/guideline_privacy-e.html.

⁴⁸ OECD Data Protection Guidelines;

<http://www.cdt.org/privacy/guide/basic/oecdguidelines.html>. The Guidelines are available for sale in book form on the OECD web site (<http://www.oecd.org/EN/home/0,,EN-home-0-nodirectorate-no-no-no-0,FF.html>) but cannot be accessed directly from the site.

⁴⁹ Data Protection Directive (95/46/EC);

http://www.europa.eu.int/comm/internal_market/privacy/index.htm.

⁵⁰ “Processing of personal data” is defined 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, consultation, use, disclosure by transmission, dissemination or otherwise making available...” Data Protection Directive, Ch.1 Art. 2, Definitions; http://www.europa.eu.int/comm/internal_market/privacy/index.htm.

⁵¹ For example, it is over the issue of EU cooperation with the U.S. Transportation Security Agency’s (TSA) requirement that European airlines turn over their records of passengers flying to the U.S. that the Computer Assisted Passenger Pre-Screening program (CAPPs II) may founder. The Data Protection Directive expressly prohibits profiling based on race, religion, and ethnicity, which records of passengers’ names and meal preferences would at least indirectly reveal. Also, the TSA’s assurances that the records will be handled according the Data Protection Directive’s standards have so far been unpersuasive. For the European Data Protection Working Party’s (Article 29) recent opinion on EU-US passenger data sharing, see http://www.epic.org/redirect/wp29_passenger_opinion.html.

⁵² See http://europa.eu.int/comm/internal_market/privacy/modelcontracts_en.htm; .pdf files of model standard contracts may be downloaded from this site.

⁵³ See, for example, the U.S. government's Web site, "International Safe Harbor Privacy Principles," dated April 19, 1999; <http://www.ita.doc.gov/td/ecom/shprin.html>. Essentially, "safe harbor" is a commitment to follow fair information practices for use of data: notice; the choice to opt-out or opt-in to use of one's data; no disclosure to third parties without notice and choice; security of data; use only for the purpose for which the data is collected (i.e., integrity of data); access and the ability to correct one's data; the right of individuals to enforce compliance with these principles against data collectors, along with sanctions for noncompliance.

⁵⁴ See "Standard contractual clauses for the transfer of personal data to third countries – FAQ"; http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=MEMO/01/228/0/AGED&lg=EN&display=.

⁵⁵ Telecommunications and Privacy Directive (97/66/EC): http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/l_024/l_02419980130en00010008.pdf.

⁵⁶ *Id.*, at Article 6 and Annex.

⁵⁷ *Id.*, at Article 3.

⁵⁸ Directive on Privacy and Electronic Communications (2002/58/EC); http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm.

⁵⁹ The other four directives related to electronic communications are the Framework, [Authorisation](#), [Universal Service](#) and [Access](#) Directives, passed in April 2002. An additional directive passed at the same time concerns radio spectrum policy.

⁶⁰ Directive on Privacy and Electronic Communications, Recital 35.

⁶¹ *Id.*, at Article 9.

⁶² *Id.*, at Articles 6 and 7.

⁶³ "Euro Parliament data retention vote upsets ISPs, telcos," Paul Meller, IDG News Service\Brussels Bureau, May 29, 2002; http://www.idg.net/ic_868587_1794_9-10000.html.

⁶⁴ Directive on Privacy and Electronic Communications (2002/58/EC), Article 15. http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm.

⁶⁵ Telecommunications Privacy Directive (97/66/EC), Article 6; http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/l_024/l_02419980130en00010008.pdf.

⁶⁶ "Majority of governments introducing data retention of communications," Statewatch (undated); <http://www.statewatch.org/news/2003/jan/12eudatret.htm>.

⁶⁷ See the Electronic Privacy Information Center's (EPIC) data retention page: http://www.epic.org/privacy/intl/data_retention.html. It has been reported in [The Register](#) (UK) that most EU countries, with the exception of Germany and Austria, support the enactment of data retention laws, even if they have not yet passed them; "Germany, Austria take stand against EU ISP data retention laws," [John Leyden](#), [The Register](#), 21/11/2002, <http://www.theregister.co.uk/content/archive/28228.html>. A November 2002 summary of member countries' data retention laws is available from the Electronic Frontier Foundation Finland: <http://www.EFFI.org/sananvapaus/eu-2002-11-20.html>.

⁶⁸ In the opinion of the UK law firm, Berwin, Leighton, Paisner, in its October 2002 Data Protection Update; http://www.blplaw.com/news/pdf_files/DataprotectionupdateOctober2002.pdf. In fact, according to Article 10 of the EC Treaty, "Member States shall take all appropriate measures, whether general or particular, to ensure fulfilment of the obligations arising out of this Treaty or resulting from action taken by the institutions of the Community. They shall facilitate the achievement of the Community's tasks. They shall abstain from any measure which could jeopardise the attainment of the objectives of this Treaty"; see Eur-Lex, [The ABC of Community Law](#), "Interaction Between Community Law and National Law," http://europa.eu.int/eur-lex/en/about/abc/abc_26.html.

⁶⁹ "European Regulators' Group agrees steps towards implementation of the New Electronic Communications Package"

http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/03/460|0|RAPID&lg=EN&display=. Another coordinating body, the 19-member Independent Regulatory Group (IRG), was set up by independent European telecommunications regulators in 1997. This group has been informally setting rules (Principles of Implementation and Best Practice, or PIBs) which its members pledge to observe in order to achieve an interpretation that is in conformity with European regulations. It is believed that ERG and IRG will merge. See http://www.regtp.de/international/start/in_11-02-00-00-00_m/.

⁷⁰ Information provided by Michael Suda, Office of the Austrian Data Protection Commission (DSK); dskpost@bka.gv.at.

⁷¹ Information provided by Anne-Christine Lacoste, Belgian Commission de la protection de la vie privée; Anne-Christine.Lacoste@privacy.fgov.be.

⁷² Information provided by Anders Sparre of Dansk-IT, a telecommunications association users group; ASP@dansk-it.dk.

⁷³ Information provided by Juhapekka Ristola of the Ministry of Transport and Communications; juhapekka.ristola@mintc.fi.

⁷⁴ Information provided by Renaud Chapelle of the Autorité de régulation des télécommunications (ART); renaud.chapelle@art-telecom.fr.

⁷⁵ Information provided by Gabriele Löwnau-Iqbal, of the Bundesbeauftragten für den Datenschutz (BfD); Gabriele.Loewnaeu-Iqbal@bfd.bund.de.

⁷⁶ Information provided by Nelius Lynch, Office of Data Protection Commissioner in Ireland, Nelius_Lynch@dataprotection.ie.

⁷⁷ Information provided by Jeroen Terstege of the Philips Corporation (Philips is not affected by the location information or data retention sections of the pending Dutch Telecommunications Act); Jeroen.Terstege@Philips.com.

⁷⁸ Information provided by Ana Isabel Martins, Portuguese Comissão Nacional Protecção Dados; amartins@cnpd.pt.

⁷⁹ Information provided by Esperanza Ballesteros of Ericsson, Spain; esperanza.ballesteros@ericsson.com.

⁸⁰ See the Electronic Privacy and Information Center's (EPIC) LSSI page: <http://www.epic.org/privacy/intl/lssi.html> (note that the link to a Babel Fish English translation does not work). The area of this law of greatest concern to civil libertarians is the requirement that all Web sites register with the government, monitor for "illicit conduct," and report it to the government; see "Web sites blackout over Spanish monitoring law," John Leyden, The Register (US), October 14, 2002, <http://www.theregus.com/content/6/26629.html>.

⁸¹ Information provided by Elisabeth Wallin, Swedish Data Inspection Board; elisabeth.wallin@datainspektionen.se.

⁸² See the UK Department of Trade and Industry's draft proposal for implementation of 2002/58/EC, "Chapter four: network and service providers' requirements – traffic data, itemised billing, calling line identification, location data services, call tracing and forwarding," p. 29; http://www.dti.gov.uk/industry_files/word/chapter_4.doc.

⁸³ Constitution of Japan, 1946, available in English at <http://www.solon.org/Constitutions/Japan/English/english-Constitution.html>.

⁸⁴ For a summary of the Act for the Protection of Computer Processed Personal Data Held by Administrative Organs in English, see <http://www.privacyexchange.org/legal/nat/omni/japansum.html>. There is no online English translation of the entire act.

⁸⁵ Controversially, the Act does not cover paper-based "koseki" family records of birth, death, marriage, divorce, and other life-cycle family events. This information is no longer publicly available, but is not considered secure. "Japan," pp. 234-241, Privacy and Human Rights 2002,

Electronic Privacy Information Center, Washington, DC. This gap has been corrected by the recently passed Personal Data Protection Law (see note 85).

⁸⁶ Personal Data Protection Law (Japanese version; English translation not yet available); <http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/030307houan.html>. Although the law was not introduced until 2001 it had been under discussion since 1999.

⁸⁷ Basic Law on the Formation of and Advanced Information and Telecommunications Network Society in 2000; http://www.kantei.go.jp/foreign/it/it_basiclaw/it_basiclaw.html.

⁸⁸ “Committee Passes Privacy Legislation,” Asahi Shimbun, 5/22/03; <http://www.asahi.com/english/politics/K2003052200326.html> and “Japan Passes Personal Information Protection Bills,” Mainichi, 5/23/03; <http://www12.mainichi.co.jp/news/mdn/search-news/881547/privacy-0-8.htm>.

⁸⁹ “Diet Enacts Personal Information Protection Laws,” Foreign Press Center/Japan; <http://www.fpcj.jp/e/shiryu/jb/0331.html>.

⁹⁰ Information in this section is derived from several newspaper articles: “New Privacy Bills Stir Up Freedom of Press Controversy,” Mainichi, 4/25/03, <http://mdn.mainichi.co.jp/news/archive/200304/25/20030425p2a00m0fp016001c.html>; “Japan Passes Personal Information Protection Bills,” Mainichi, 5/23/03, <http://www12.mainichi.co.jp/news/mdn/search-news/881547/privacy-0-8.htm>; “Diet Passes Landmark Set of 5 Bills to Protect Personal Information,” Yomiuri Shinbun, <http://www.yomiuri.co.jp/newse/20030524wo01.htm>; “Privacy Now Better Protected,” Yomiuri Shinbun, 5/24/03, <http://www.yomiuri.co.jp/newse/20030524wo81.htm>.

⁹¹ Information and translation provided by Ema Tanaka, Researcher in Info-Communications; Research Institute of Telecommunications and Economics (Japan); ema@rite-i.or.jp.

⁹² “Guidelines on the Protection of Personal Data in Telecommunications Business”; http://www.soumu.go.jp/joho_tsusin/whatsnew/guideline_privacy-e.html.

⁹³ *Id.*, Article 1.

⁹⁴ *Id.*, Article 8.

⁹⁵ *Id.*, Article 11.

⁹⁶ Basic Law on the Formation of and Advanced Information and Telecommunications Network Society in 2000; http://www.kantei.go.jp/foreign/it/it_basiclaw/it_basiclaw.html.

⁹⁷ Mobile Media Japan’s web site updates these 3G and mobile Internet subscriber figures regularly; <http://mobilemediajapan.com>.

Sources

Statutes, Regulations, Legislation and proposed legislation:

United States

47 U.S.C. 222, 251, Telecommunications Act of 1996; as amended by the Wireless Communications and Public Safety Act of 1999 (WCPSA).

California Public Utilities Commission, “Telecommunications Consumer Bill of Rights” (draft); <http://www.cpuc.ca.gov/static/Industry/Telco/billofrights.htm>.

HR 122, “Wireless Telephone Spam Protection Act,” 108th Congress; <http://thomas.loc.gov>.

HR 71, “The Wireless Privacy Protection Act,” 108th Congress; <http://thomas.loc.gov>.

Implementation of the Telecommunications Act of 1996; Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information, CC Docket No. 96-

115, FCC 02-214; June 23, 1998; http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-214A1.pdf.

In the Matter of the Request by the Cellular Telecommunications and Internet Association to Commence Rulemaking to Establish Fair Information Practices, WT Docket No. 01-72, FCC 02-208; July 24, 2002; http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-208A1.doc.

Links to state DMCA laws are on Professor Edward Felton's Freedom to Tinker web site; <http://www.freedom-to-tinker.com/superdmca.htm>

Motion Picture Association of America (MPAA), "Draft Model Communications Security Legislation"; http://www.freedom-to-tinker.com/doc/2003/mpaa_3apr.rtf

S 1164, "Location Privacy Protection Act," 107th Congress: <http://thomas.loc.gov>.

Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, CC Docket No. 96-115, FCC 98-27; Final Rule; released Feb. 26, 1998; http://www.fcc.gov/Bureaus/Common_Carrier/Orders/1998/fcc98027.txt.

Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, CC Docket No. 96-115; FCC 01-247; Clarification Order and Second Notice Further Notice of Proposed Rulemaking; ¶ 7 (CPNI Clarification Order); http://www.fcc.gov/Bureaus/Common_Carrier/Orders/1998/fcc98027.txt.

European Union

Data Protection Directive (95/46/EC); http://www.europa.eu.int/comm/internal_market/privacy/index.htm.

Directive on Privacy and Electronic Communications (2002/58/EC); http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm.

Electronic Frontier Foundation Finland, summary of EU member countries' data retention laws; <http://www.effi.org/sanavapaus/eu-2002-11-20.htm>.

Electronic Privacy Information Center (EPIC) data retention page: http://www.epic.org/privacy/intl/data_retention.htm.

Electronic Privacy and Information Center (EPIC) LSSI (Spain's "Law of Information Society Services and Electronic Commerce") page; <http://www.epic.org/privacy/intl/lssi.html>.

Eur-Lex, The ABC of Community Law, "Interaction Between Community Law and National Law," http://europa.eu.int/eur-lex/en/about/abc/abc_26.html.

OECD Data Protection Guidelines; <http://www.cdt.org/privacy/guide/basic/oecdguidelines.html>.

Telecommunications and Privacy Directive (97/66/EC): http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/l_024/l_02419980130en00010008.pdf.

UK Department of Trade and Industry's draft proposal for implementation of 2002/58/EC; http://www.dti.gov.uk/industry_files/word/chapter_4.doc.

Japan

Act for the Protection of Computer Processed Personal Data Held by Administrative Organs (English summary; no complete English translation available online); <http://www.privacyexchange.org/legal/nat/omni/japansum.html>.

Basic Law on the Formation of and Advanced Information and Telecommunications Network Society in 2000; http://www.kantei.go.jp/foreign/it/it_basiclaw/it_basiclaw.html

Constitution of Japan, 1946 (in English); <http://www.solon.org/Constitutions/Japan/English/english-Constitution.html>.

Guidelines on the Protection of Personal Data in Telecommunications Business, Ministry of Posts and Telecommunications, Japanese Government December 2, 1998; Article 11, no. 1; http://www.soumu.go.jp/joho_tsusin/whatsnew/guideline_privacy-e.html.

Personal Data Protection Law (in Japanese version; English translation not yet available); <http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/030307houan.html>.

Cases:

U.S. v. Miller, 435 U.S. 425 (1976)

U.S. West v. FCC, 182 F.3d 1224 (10th Cir.1999); (cert. denied, 530 U.S. 1213, June 5, 2000)

Individual Sources:

Ballestros, Esperanza, Ericsson, Spain; esperanza.ballesteros@ericsson.com.

Chapelle, Renaud of the Autorité de régulation des télécommunications (ART); renaud.chapelle@art-telecom.fr.

Ishikawa, Yutaka, LL.M. student in International law, Chuo University, Tokyo; wakashi@tkg.att.ne.jp.

Lacoste, Anne-Christine, Belgian Commission de la protection de la vie privée; Anne-Christine.Lacoste@privacy.fgov.be.

Löwnau-Iqbal, Gabriele, Bundesbeauftragten für den Datenschutz (BfD); Gabriele.Loewnau-Iqbal@bfd.bund.de.

Lynch, Nelius, Office of Data Protection Commissioner in Ireland; Nelius_Lynch@dataprotection.ie.

Martins, Ana Isabel, Portuguese Comissão Nacional Protecção Dados; amartins@cnpd.pt.

Sparre, Anders, Dansk-IT, a telecommunications association users group; ASP@dansk-it.dk.

Ristola, Juhapekka, Ministry of Transport and Communications; juhapekka.ristola@mintc.fi.

Suda, Michael, Office of the Austrian Data Protection Commission (DSK); dskpost@bka.gv.at.

Tanaka, Ema, Researcher in Info-Communications; Research Institute of Telecommunications and Economics (Japan); ema@rite-i.or.jp.

Terstegge, Jeroen, Philips Corporation (Netherlands); Jeroen.Terstegge@Philips.com.

Wallin, Elisabeth, Swedish Data Inspection Board; elisabeth.wallin@datainspektionen.se.

Articles:

“AT&T Wireless Helps Callers Find Friends,” PCWeek, 6/26/02;
http://www.pcworld.com/news/article/0_aid,102269,00.asp.

“Auto-ID: Tracking everything, everywhere [RFID],” Katherine Albrecht;
<http://www.nocards.org/AutoID/overview.shtml>.

“Committee Passes Privacy Legislation,” Asahi Shimbun, 5/22/03;
<http://www.asahi.com/english/politics/K2003052200326.html>.

“Diet Enacts Personal Information Protection Laws,” Foreign Press Center/Japan;
<http://www.fpcj.jp/e/shiryu/jb/0331.html>.

“Diet Passes Landmark Set of 5 Bills to Protect Personal Information,” Yomiuri Shinbun,
<http://www.yomiuri.co.jp/newse/20030524wo01.htm>.

“Euro Parliament data retention vote upsets ISPs, telcos,” Paul Meller, IDG News Service\Brussels Bureau, May 29, 2002; http://www.idg.net/ic_868587_1794_9-10000.html.

“Germany, Austria take stand against EU ISP data retention laws,” John Leyden, The Register, 21/11/2002, <http://www.theregister.co.uk/content/archive/28228.html>.

IETF: “Geopriv Requirements,” Jorge Cuellar, John B. Morris, Jr. (Center for Democracy and Technology), Deirdre Mulligan (Samuelson Law, Technology, and Public Privacy Clinic), Jon Peterson (NeuStar), James Polk (Cisco); March 2003 draft;
<http://www.ietf.org/internet-drafts/draft-ietf-geopriv-reqs-03.txt>.

“Japan Passes Personal Information Protection Bills,” Mainichi, 5/23/03;
<http://www12.mainichi.co.jp/news/mdn/search-news/881547/privacy-0-8.htm>.

“Majority of governments introducing data retention of communications,” Statewatch (undated);
<http://www.statewatch.org/news/2003/jan/12eudatret.htm>

“New Privacy Bills Stir Up Freedom of Press Controversy,” Mainichi, 4/25/03,
<http://mdn.mainichi.co.jp/news/archive/200304/25/20030425p2a00m0fp016001c.html>.

“Privacy Now Better Protected,” Yomiuri Shinbun, 5/24/03,
<http://www.yomiuri.co.jp/newse/20030524wo81.htm>.

“RIAA takes aim at individual swappers; Group will seek subscriber info from ISPs,” Paul Roberts, IDG News Service, 6/25/03;
http://www.infoworld.com/article/03/06/25/HNriaaim_1.html?networking.

Warren, Samuel, and Brandeis, Louis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 213 (1890).

Press Releases:

“European Regulators’ Group agrees steps towards implementation of the New Electronic Communications Package”

http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/03/460/0|RAPID&lg=EN&display=.

“FCC Adopts Rules Resolving How Phone Companies Share and Market Customer Information,” FCC News, 7/16/02, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-224366A1.doc.

“Washington [State] regulators adopt nation’s strongest telephone customer-privacy rules,” Nov. 7, 2002;

<http://www.wutc.wa.gov/webdocs.nsf/6f0baa33f074e151882566c20000604d/93d4130392518ad988256c6a0060f5a5>.

Miscellaneous:

Cellular Telecommunications and Internet Association’s web site wireless subscriber counter; <http://www.wow-com.com/>.

Electronic Privacy Information Center (EPIC) complaint to the FTC to enjoin DoubleClick’s online profiling practices and alleging that the company had violated its own privacy policy; http://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf.

EU Data Protection Directive-compliant model standard contracts; http://europa.eu.int/comm/internal_market/privacy/modelcontracts_en.htm.

“International Safe Harbor Privacy Principles,” dated April 19, 1999; <http://www.ita.doc.gov/td/ecom/shprin.html>.

Mobile Media Japan’s web site 3G and mobile Internet subscriber counter; <http://mobilemediajapan.com>.

October 2002 Data Protection Update, Berwin, Leighton, Paisner (UK law firm); http://www.blplaw.com/news/pdf_files/DataprotectionupdateOctober2002.pdf.

Petition of the Cellular Telecommunications Industry Association for a Rulemaking to Establish Fair Location Information Practices; <http://www.cdt.org/privacy/issues/location/001122ctia.pdf>.