Privacy and Mobile Telecommunications

KURT WIMMER

It's easy enough to imagine the consumer benefits that might flow from technologies that track the location of mobile phone users, especially in situations like the following:

• Your purse has just been stolen. Your partner's one-button mobile call to an emergency service immediately pinpoints your location for the police, and the mobile phone inside the purse allows them to quickly track down the culprit.

• You're trying to choose among several coffee shops in your neighborhood. Your mobile phone produces an electronic coupon for great savings on a Sumatran blend. The coupon helps you choose and helps your local merchant diminish his inventory of an overstocked brand.

• On a dark night, you are in a taxi, running late for an important appointment, and your driver needs directions; a mobile phone with location monitoring can provide alternate routes and estimated travel times.

It is just as easy to contemplate the difficulties with mobile location technologies. Your always-on mobile phone produces a signal that allows the police to follow your every movement with pinpoint precision. The same sort of electronic coupon that you welcome at a favorite neighborhood shop becomes a real nuisance when you are constantly besieged by scores of merchants eager to sell their wares through your mobile phone.

New laws on data privacy and limits on the reach of law enforcement may provide a framework that will permit the benefits of these technologies while minimizing the drawbacks, at least in some countries. Technology often outpaces the legal system, but there is a good chance that mobile location technologies may fit into existing principles for consumer choice and privacy in a way that many others do not.

Kurt Wimmer (kwimmer@cov.com) is a partner in the London, England, office of Covington & Burling.

This article provides a very brief overview of data privacy principles in Europe and those under consideration in the United States, as well as principles binding on law enforcement authorities in the U.S. and the United Kingdom. The article concludes that mobile location technologies should be deployed with a system of consumer choice that complies with data privacy principles. Ironically, European telecommunications users enjoy great protection against commercial exploitation of their privacy but less protection against law enforcement incursions into their personal data.

Privacy from Companies, Privacy from the State

Privacy, as a legal concept, is not easily or universally defined. In the context of mobile location technologies, the word has two distinct meanings. The first is really information privacy, the protection of elements of life from others that gives rise to rules governing the collection and maintenance of personal data, sometimes called "data protection."[1] The second is more akin to the protection of private communications from the state—the ability to keep various forms of communications from law enforcement under rules regulating police searches and seizures.[2]

The first type of privacy, data protection, is most relevant to the behavior of network operators and other companies providing mobile location services. The emerging international law of data protection typically focuses on five factors: notice, choice, access, security, and enforcement. Consumers should have notice that information about them is being collected, a choice about whether it should be collected or not, access to information that has been collected about them, security that the data is being held beyond the reach of anyone not entitled to hold it, and enforcement of these obligations. These factors are drawn from European law, which has a heritage of treating privacy as a fundamental human right, and particularly from the European Union's Data Protection Directive and the 1980 Organization for Economic Cooperation and Development privacy guidelines.[3]

The second type of privacy, protection of personal data from the state, has its roots in constitutional law in the United States and a few other countries, international treaties and conventions, and long-standing statutory restrictions on the appropriate actions of the state in other countries.[4] In the United States, this body of law is rooted in the Fourth Amendment, and was extended to protection against wiretaps in the landmark case of *Katz v. United States*.[5] As technology has progressed, these rights have become more contentious and the dividing lines more blurred. In another, more recent case, *Kyllo v. United States*, the U.S. Supreme Court found that police must obtain a search warrant before using high-tech methods such as thermal imaging devices to determine the contents of a home.[6] Specifically, the five-four majority opinion in *Kyllo* held that where "the Government uses a device that is not in general public use to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a Fourth Amendment 'search' and is presumptively unreasonable without a warrant."[7] This case has led to questions of whether government use of other technologies, including the Carnivore system for sifting and tapping Internet communications, is constitutional.[8]

Limits on Commercial Treatment of Data

Consumers and communications practitioners are most familiar with data protection principles from considering website privacy policies. Who can collect your data? What can they do with it? Can they use it only for their own purposes, or sell it to others? How do you provide consent on how it should be used—by positive, opt-in consent to

specific uses, or by agreeing to opt out of any uses you don't like? How can you access data held on you by a website, and who enforces these rules?

Europe—Pervasive Regulation

In Europe, these principles have been in place for years. Under the European Union's Data Protection Directive, and the EU member state laws that have been passed to implement that directive, European citizens have significant rights to the privacy of personally identifiable data about them.

The directive imposes rules on "data controllers," the people and companies who oversee the use and transfer of personally identifiable information, if they are either located or use equipment in the EU. Data controllers must register their activities with a supervisory authority in the EU member state in which they are operating. In addition, the directive:

- specifies the rights that individuals have with respect to personal data held by others;
- establishes special obligations for sensitive information;
- includes specific provisions regarding enforcement; and
- imposes significant restrictions regarding the transfer of personal data from EU member states to non-EU countries.

The directive does not, however, directly regulate privacy in each European country. Rather, each EU member state is obligated by treaty to pass a national law implementing the directive. Although these laws vary somewhat, they are bound by treaty to contain the essential elements of the EU directive they are seeking to implement. Data protection laws have been passed by the fifteen EU member states as well as seventeen other countries.[9] The United Kingdom implemented the EU Data Protection Directive by passing the Data Protection Act (1998).[10] This Act demonstrates how data protection principles may be applied to mobile location technologies.

The essential issue, of course, is whether a subscriber's physical location qualifies as "personal data." Personal data means information relating to a living individual who can be identified from either the data themselves or from the combination of that data with other information that is held by the data controller. There is a very good chance that mobile location information will be seen as "personal data" for purposes of the law. The fact that subscribers are in a particular physical location does reveal some personal information about them, and that information can be combined with data held by the mobile phone carrier to reveal both their identities and whereabouts. Indeed, location information could qualify as specifically protected "sensitive personal data," information relating to an individual's race or ethnicity, political opinions, religious beliefs, sexual life, physical or mental health, or trade union membership.

Once it has been determined that location information is personal data, specific obligations attach to its collection, transfer, and maintenance. The data may be obtained and processed only for specific purposes. For example, a credit card company can use data on an individual's purchasing habits to extend credit but not, without further consent, to create a profile of the consumer's favorite kinds of merchandise. The data cannot be excessive in relation to the purpose for which it is collected, i.e., the number called and the length of a call might be recorded by a telephone company for billing purposes, but the content of the call certainly could not be. The data must be accurate, and held only as long as necessary for their purpose. For example, call information relating to billing should not be held after the account has been paid.[11] The integrity and security of the information must be assured, and the data cannot be transferred to a non-EU country unless that country has equivalent protections for personal data.

The real crux of the matter is that the data must be processed "fairly," which requires that the consumer provide effective consent. That means that the individual must have access to information about the identity of the data controller, the purpose for which the data will be collected and processed, and "any further information which is necessary, having regard to the specific circumstances in which the data is to be processed, to enable processing in respect of the data subject to be fair."[12] Although each company should make this determination in light of the purpose for which the mobile location data are collected, it seems likely EU rules will require prior consent of the subscriber. This prior consent, moreover, will need to include accurate information on how the company will collect the information; what information will be collected and how it will be used; and to whom the information might be provided (third-party contractors, advertisers, and the like). In Europe, prior, specific consent is required, and consumers must opt in to any planned data collection program.[13]

Importantly, the European Union is considering the adoption of a specific, new directive on data protection in the electronic communications sector. This directive deals specifically with location data and provides that it may be used only with the specific consent of the subscriber. The subscriber also must be able to temporarily suspend the collection of location information—that is, even if the handset is an "always on" handset, the subscriber must be able to override any location monitoring technologies operating within the handset. This is a familiar principle in Europe because of a parallel requirement imposed on caller identification; handsets must be able to block the transfer of information about the subscriber on a call-by-call basis. It appears, based on current language being debated in the European Parliament, that this directive will require full prior consent from consumers before the collecting of any personally identifiable location information:

> Where electronic communications networks are capable of processing location data other than traffic data, relating to users or subscribers of their services, this data may be collected, stored, and processed only when identifiers have been removed, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value-added service specifically requested by the user.[14]

This new directive is likely to be passed by the end of 2001; member states will then have a period, probably eighteen months, to enact legislation to implement the directive.[15]

The American Experience

In the United States, there is very little specific regulation of consumer data. Unlike the case in Europe, where privacy is regulated generally and specific types of information collection and processing fit into those general regulations, U.S. law tends to deal separately with each specific type of information collection. For example, specific legis-

lation has been required to protect financial services information, health care information, Internet data relating to children, cable television and telecommunications subscription data, and even information on videotapes a customer may have rented.[16] No general, overarching law regulates privacy generally and provides a ready framework for the collection and processing of mobile location data.

In this legal context, a specific regulatory proposal likely will be needed if policymakers wish to address the privacy of location information. However, the Cellular Telecommunications and Internet Association (CTIA) has filed a petition for rulemaking with the Federal Communications Commission, suggesting that the FCC craft "fair location information practices."[17] Although it seems counterintuitive, in some ways, for an industry to seek federal regulation of a new business practice, CTIA's action is a logical one. First, the establishment of rules by the FCC could dissuade Congress from passing more comprehensive legislation to regulate location monitoring. Second, FCC rules could prevent individual states from creating a patchwork quilt of inconsistent regulations and thwarting the growth of a new service.

These practices would, in some sense, be based on the European standards for data protection: the suggested standards would require notice and consent by the subscriber before any location information is disclosed or used by the carrier. The CTIA proposes a more flexible structure for obtaining prior consent: it suggests that carriers might obtain subscribers' consent in a number of different ways, and it takes no position on whether consent must be opt-in, as would be the case in Europe, or opt-out.[18] The CTIA also suggests that any information obtained should be collected and maintained securely to protect against unauthorized access and disclosure. It does not, however, suggest a general "access" provision under which consumers could review information held on them by carriers because "most location information is ephemeral and kept only to complete a transaction." If, however, profiles are created, CTIA supports a subscriber right of access to correct any inaccuracies.[19] Although CTIA does not suggest an explicit enforcement mechanism, any set of obligations established by the FCC could be enforced by the agency.

The FCC has opened a docket and has received comments on the CTIA petition. No action has so far been taken. Since the petition was filed, the composition of the FCC has changed dramatically because several new commissioners have been appointed by the Bush administration, and it remains unclear what the stance of the current FCC will be toward establishing privacy rules.

Even though telecommunications carriers' obligations toward subscribers on location privacy are not yet clear, other FCC proceedings reveal that carriers soon will have the capability to precisely determine the location of subscribers. These developments are occurring to assist emergency services in locating wireless subscribers who call for help. As Thomas Sugrue, the chief of the FCC's Wireless Telecommunications Bureau, told Congress in June 2001, security is a major reason for the increase in American use of wireless technologies. "But that help may never arrive, or may be too late, if the 911 call does not get through or if emergency response teams cannot locate you quickly."[20] The FCC has issued a series of orders over the past five years establishing a method for emergency services to determine the location of callers of 911 emergency services.[21] Congress also passed the Wireless Communications and Public Safety Act in 1999.[22]

Law enforcement agencies have been just as focused on these new technologies' capability to help apprehend criminals.

These enhanced 911, or E911, requirements have several stages. At the most basic level, the FCC requires emergency calls to be routed to a central processing center and to be transmitted without regard to validation of the caller's status as a subscriber. At the more advanced level, the FCC will require carriers to provide location information of all wireless 911 callers to these processing centers. The Phase I rules require carriers to provide information on the base station handling the call, which may narrow down the location of the caller to a few city blocks in a dense area or a few miles in the case of a rural analogue cellular system. The Phase II rules, which take effect in October 2001, will require carriers to provide location information with much greater precision. According to the FCC timetable, U.S. wireless carriers will have significant mobile location capabilities by 2005.

The State Interest

Commercial services have been carefully watching the evolution of location monitoring technologies. But law enforcement agencies have been just as focused on these new technologies' capability to help apprehend criminals.

In response to concerns expressed by the Federal Bureau of Investigation that new telecommunications technologies could thwart criminal investigations, Congress passed the Communications Assistance for Law Enforcement Act (CALEA).[23] During the brief congressional debate leading up to CALEA's passage, then-FBI Director Louis Freeh stated that the FBI did not wish to turn wireless phones into location-tracking devices. "There is no intent whatsoever," he testified, "to acquire anything that could properly be called 'tracking information.' "[24] Yet in implementing CALEA, the FCC agreed to permit law enforcement agencies such as the FBI to have access to callers' locations at the beginning and end of each call; this ruling was upheld by the District of Columbia Circuit last summer.[25] Importantly, however, the court indicated that law enforcement would need more than a mere pen-register order—an order that can be obtained without a search warrant.[26]

In the United Kingdom, the Regulation of Investigative Powers Act (known by the unfortunate acronym RIP Act) came into force in October 2000 and regulates government access to electronic communications. The RIP Act provides that police no longer need to get a warrant issued by the Home Secretary to intercept and read electron-

ic communications. Now, a warrant can be issued by a police superintendent, who may then order the disclosure of mobile position information concerning a suspect, not only at the beginning and end of a call, as is the case in the United States, but throughout its duration. Under the RIP Act, mobile location information will be available broadly to law enforcement without a judicial or even administrative search warrant.

The laws of other countries will, of course, establish other standards. Some may provide greater protection than the United States and United Kingdom; others may provide less protection or act in a less transparent manner. Telecommunications carriers in each country—and, perhaps with even more difficultly, carriers that act in multiple jurisdictions—may thus need to inform consumers that their privacy will be subjected to a variety of legal schemes.

Conclusion

Mobile location technologies promise a dramatic improvement in the safety and convenience available to subscribers to wireless telecommunications services. Yet consumers may be less than enthusiastic to subscribe to these services without adequate assurances for their privacy. Consumers clearly are concerned about securing their privacy against commercial interests obtaining or revealing location information without their consent. Potential subscribers may be less aware of threats to their privacy pursuant to law enforcement efforts, but one might legitimately expect these issues to be raised by privacy advocates and others as these technologies become more robust and widely available. The burden of demonstrating adequate assurances for privacy likely will fall upon mobile telecommunications carriers wishing to offer these services to their subscribers, whether in Europe or the United States.

Endnotes

1. *See* DAVID BANISAR & SIMON DAVIES, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS 3 (2000).

2. *See id.* This branch of "privacy" has its roots in organic laws such as the U.S. Constitution and even older laws such as the 1361 Justice of the Peace Act in England. Even before the U.S. Constitution was drafted, British law protected family homes from unreasonable searches and seizures. In 1765, Lord Camden struck down a warrant to enter a home, stating that "[w]e can safely say there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society, for papers are often the dearest property any man can have." Entick v. Carrington, 1558–1774 All E.R. Rep. 45, *quoted in* BANISAR & DAVIES, *supra* note 1. This principle was, of course, followed in U.S. constitutional law. *See, e.g.*, Smith v. Maryland, 442 U.S. 735 (1979).

3. Directive of the European Parliament and the Council of Europe on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (July 20, 1995); Organisation for Economic Co-Operation and Development Recommendation Concerning the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (Sept. 23, 1980).

4. *See, e.g.*, United Nations General Assembly, Universal Declaration of Human Rights, Article 12 (1948) ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence"); Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8 (1950) ("Everyone has the right to respect for his private and family life, his home and his correspondence").

5. 386 U.S. 954 (1967).

6. No. 99–8508 (June 2001), *rev'g* 190 F.3d 1041 (9th Cir. 1999).

7. *Id.* Interestingly, the majority opinion in *Kyllo* was written by Justice Scalia, not ordinarily in the majority in Fourth Amendment cases striking down government actions as unconstitutional searches. His leadership in this case could be explained by the fact that *Kyllo* involved a home.

8. *See, e.g.*, Letter from Dick Armey, Majority Leader, U.S. House of Representatives, to John Ashcroft, Attorney General, United States, June 14, 2001 (available at http://freedom.house.gov/library/technology/ashcroftletter.asp).

9. *See* Stewart Dresner, *Privacy: The Impact of the EU's Proposed E-Com Directive on Mobile Location Services, in* EUROFORUM, MOBILE LOCATION SERVICES 2001 (2001).

10. Data Protection Act 1998, *available at* www.hmso.gov.uk/acts/acts1998/19980029.htm.

11. This requirement could lessen the commercial viability of archived location information but the major commercial use for location information is at the moment of collection.

12. Data Protection Act 1998, Schedule 1, Part 2.

13. Some telecommunications users may be required to give up rights of privacy as a condition of employment. To the extent that employees have a right of privacy in their whereabouts during the workday, they may be required to sign that right away to permit their employer to manage the movement of their employees and vehicles (and, by extension, to monitor their employees' work habits).

14. *See* European Parliament, Opinion of the Committee on Industry, External Trade, Research and Energy on the Proposal for European Parliament and Council Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector 15 (2000/0189 (COD) June 14, 2001).

15. *See id.*

16. *See, e.g.*, 47 U.S.C. § 631 (cable services data); 47 U.S.C. § 222 (telecommunications services data); 18 U.S.C. § 2710 (video rental data).

17. *See* Petition of the Cellular Telecommunications Industry Association for a Rulemaking to Establish Fair Location Information Practices (WT Docket 01–72, filed Nov. 22, 2000). The CTIA has, since filing the petition, changed its name to the Cellular Telecommunications and Internet Association.

18. *See id.* at 9. The suggestions for permissible notice that CTIA suggests include a provision in a general subscriber agreement, the service provider sending an e-mail message or letter describing the services, or a bill insert describing the location practices of the carrier referring the subscriber to a website. *Id.* at 9 and 9 n.23.

19. *See id.* at 10–11.

20. *Hearing on Wireless E-911, House Subcomm. on Telecommunications, Trade and Consumer Protection, Committee on Commerce,* 107th Cong., 1st Sess. (June 14, 2001) (statement of Thomas J. Sugrue, Chief, Wireless Telecommunications Bureau, Federal Communications Comm'n).

21. *See* the FCC's website at www.fcc.gov/e911/factsheet_requirements_012001.txt.

22. Pub. L. No. 106–81, enacted October 26, 1999, 113 Stat. 1286, amending the Communications Act of 1934, 47 U.S.C. §§ 222, 251.

23. For a comprehensive overview of the passage and implementation of CALEA, *see* David Sobel, *Privacy and Law Enforcement in the Digital Age*, 18 COMMUNICATIONS L., at 3 (Winter 2001).

24. *See Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375,* 103d Cong., 2d Sess. at 29 (1994) (statement of Louis Freeh, Director, Federal Bureau of Investigation).

25. *See* United States Telecommunications Ass'n v. Federal Communications Comm'n, 227 F.3d 450 (D.C. Cir. 2000).

26. *See id.* at 453.