



March 17, 2010

Privacy

Location Privacy Advocates Draw Lessons From European, Industry-Based Approaches

by *Christine Mumford*

Location Privacy Advocates Draw Lessons From European, Industry-Based Approaches

Cell phones and mobile devices are increasingly able to provide accurate, precise location-based information on users simply and at relatively low cost, prompting lawmakers and others to wonder whether — and how — location services should be federally regulated.

Last month, Rep. Rick Boucher (D-Va.) said he is considering including location-based privacy sections in privacy legislation he is drafting (15 ECLR 317, 3/3/10). Federal privacy legislation has been slow in coming, however. Many states have been active in drafting and passing privacy legislation, and while generally applicable federal legislation is frequently proposed, it has had difficulty garnering the support necessary to become law (13 ECLR 1166, 8/27/08).

The reasons for the impasse are familiar and longstanding: Privacy advocates press for a legislative solution, while businesses promote self-regulation.

Part of the problem may be that “privacy” is so broad a concept. Privacy legislation would include data breaches, restrictions on health and other sensitive personal data, and behavioral tracking online, among other things.

European law could offer a way forward for the United States, but there are problems with that approach as well. The European Union’s directive is differently implemented in each member state, for instance, causing at least pause for multinational telecommunications companies. And the directive’s definitions are fixed and the amendment process long, making updates to account for changes in technology or data usage unlikely.

Location-based privacy was touched on by Congress in the 1999 Wireless Communications and Public Safety Act. The act authorizes the provision of “call location information concerning the user of a commercial mobile telephone service,” but is limited to instances of 911 emergency calls unless the wireless carrier has obtained “the express prior authorization of the customer” to use the data for other purposes. The contours of that authorization and scope of the “other uses” implicated is undeveloped.

Lawmakers looking to draft more specific privacy and data protection guidelines may be able to find some guidance by looking to the European Union. The EU has, since 2002, required

member states to implement location-based privacy protections for communications other than emergency calls.

The Electronic Privacy Information Center, a Washington, D.C.-based public interest research group, submitted a statement to the House Energy and Commerce Committee Feb. 24 urging that any privacy directive include location-based privacy rules mirroring the European policies.

“Concerns regarding locational privacy are arising in other countries,” EPIC’s president Marc Rotenberg said. “The responses in Europe, in particular, provide the United States with a possible model to protect the privacy of locational data.”

Rotenberg said that the European approach could be a good model here, particularly as it relates to consent, and how consent is obtained. The European Union requires opt-in consent, the contours of which it sets out in some detail.

“Mobile devices have become ubiquitous in modern society and their use has become common among younger and younger children,” Rotenberg said. “In light of this, it is important that clear standards are formulated in order to protect the privacy of users by giving the users control over their own data and requiring an opt-in model for the use of this data,” he said. He saw the European approach as a workable model as the United States looks to draft more pointed regulation.

European Opt-In Model.

Under the 2002 Directive on Privacy and Electronic Communications (2002/58/EC), the European Union requires telecommunications operators and internet service providers in all member states to obtain consent before collecting or using customer location data.

That directive, known as the E-Privacy Directive, built upon the principles of the 1995 Data Protection Directive (95/46/EC). It is entirely separate from the Universal Service Directive, 2002/22/EC, which sets parameters for location information disclosure in the case of emergency calls.

The Data Protection Directive requires member states to regulate the processing and free movement of personal data. The E-Privacy Directive adds requirements for “publicly available electronic communications services,” including a requirement that the processing of location data other than traffic data be done either (a) anonymously; or (b) with the consent of the affected users or subscribers.

“Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, 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,” the E-Privacy Directive stipulates.

“The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service.”

The directive also provides that users and subscribers must be given the possibility to withdraw their consent at any time, even on a case-by-case basis.

Under the directive, consent may be given by “any appropriate method enabling a freely given specific and informed indication of the user’s wishes.” The directive stipulates that this could include “ticking a box when visiting an internet website.”

Differences of National Law

The interpretation of what consent actually means in any given situation would be a question of national law, however. The E-Privacy Directive, like all EU Directives, provides the framework for the member states, but the member states themselves are ultimately responsible for implementing the directives into their own system of national laws. The directive is thus not as straightforward as its text might indicate, David Taylor, a partner at Lovells Paris, told BNA.

“The very nature of directives — which set minimum standards to be complied with by all member states but leaves them to pass local legislation — means that inconsistencies and differences of treatment across Europe are inevitable,” Taylor said. “Data protection legislation therefore varies depending on member states and legislative cultures.”

Countries like France and Spain have more stringent requirements than countries like the UK, Taylor said. Telecommunications operators doing business across Europe must look not just to the directive, but also to the specific requirements of each national law.

“In principle, telecommunications operators remain under the obligation to obtain express consent from their clients to process location information, and such consent is often collected both at the time of subscription to a contract but also when the client is about to use a service of that nature with a message requesting consent,” Taylor said. Data storage, he said, is dependent on the technical choices of the telecommunications operators. So long as their choices comply with the directive as implemented in each state, the telecommunications operators are free to make their own storage choices, he said.

Consistency Concerns for Telecoms

The differences in member state law do place a burden on operators, Jörg Hladjk, a lawyer at Hunton & Williams in Brussels, told BNA.

“What may constitute consent may for example differ from country to country, but not too dramatically,” Hladjk said. “There are specific particularities in some countries, and from a multinational company’s perspective, all laws must be considered,” he said. “But because of the

directive, all laws look mostly the same if the member states implemented the directive properly.”

There is no such semblance of uniformity in the United States, where privacy is legislated on a strictly state level without the benefit of any over-arching guidelines. State privacy laws have not, as of yet, included location-based privacy considerations. When and if they do, the ease of operating in multiple jurisdictions may become a pressing issue.

At least in the European Union, a coordinating body has been a very useful tool for handling the differences of interpretation and implementation, both Hladjk and Taylor said.

“In cases where issues have arisen because of the differences of implementation and approaches, the work of the Article 29 Working Party has been extremely useful to try to define common approaches by the local data protection authorities,” Taylor said.

The Article 29 Working Party is a product of the Data Protection Directive. It is a group of advisors from across the EU that offers advice on various EU law initiatives, and explains enforcement mechanisms to member states and citizens.

The working party published, in 2005, an opinion paper providing additional insight into how telecommunications operators should approach issues of consent and data storage on a wider, pan-European level. The paper, “Opinion on the use of location data with a view to providing value-added services,” is a “very valuable resource,” according to Hladjk.

“If companies have questions or issues on processing or providing services, they can turn to the working party document,” Hladjk said.

The paper is of an advisory nature only, and is non-binding. It provides insight into how data protection authorities think on a more practical level, however, and gives indications how enforcement could happen — information Hladjk called invaluable.

Directive’s Limitations

One potential limitation of the EU approach is its applicability: The E-Privacy directive very clearly only applies to communications sent over “public communications networks.”

“Communication” is defined in Article 3 of the directive to mean “any information exchanged or conveyed between a finite number of parties by means of a publicly available communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network, except to the extent that the information can be related to the identifiable subscriber or user receiving the information.” Contractors would be covered, at least in terms of collecting consent, under recital 32.

“The directive is limited to telecoms operators and ISPs,” Hladjk said. “It was developed to cover the data processing in the specific sector of electronic communications,” he said.

The directive's definitions are not likely to change. The European Union at the end of 2009 completed revisions on the E-Privacy directive, but its primary focus was data breach notice. "The amendments were a very long process, and the existing regime on location data was essentially untouched," Hladjk said. "Therefore, location privacy is not a topic that the EU seems likely to pick up again soon."

The changes in technology and the growing uses for location information may demand a more plastic framework for dealing with the privacy implications location data use, public advocacy groups have said (15 ECLR 317, 3/3/10).

According to Michael Altschul, senior vice president and general counsel of CTIA--The Wireless Association, industry-driven best practices may be a better way to address privacy than legislation that could, after a time, grow outdated or overly limited. CTIA is an industry association for wireless telecom companies.

Altschul told BNA that industry guidelines like CTIA's 2008 "Best Practices and Guidelines for Location-Based Services" would be a "very workable" alternative to legislation.

"When the Wireless Communications and Public Safety Enhancement Act of 1999 was passed, there was a widely held assumption that location-based services would involve a wireless carrier having access to a user's location information and then using or sharing that information to provide a location-based service," Altschul said. But anymore, he said, location technologies involve a whole host of players. Altschul listed the increased reliance on smartphones, the "rapid evolution" towards open platforms, and the increasing use of GPS services that can be downloaded and enabled without wireless carriers' knowledge, as among recent advancements.

A benefit of the guidelines, he said, is that they can be changed and updated without the burdens of legislative amendment. He said that CTIA is currently making changes to its guidelines, which he said most players in the wireless industry have committed to--and do--follow.

"While the new guidelines have yet to be finalized, they will balance public safety's needs with consumers' privacy," he said.

The only place Altschul saw a real need for Congressional intervention was with respect to public safety, and law enforcement's ability to efficiently access location-based data.

"As technology continues to evolve, we would encourage Congress to clarify the terms under which location information may be released to law enforcement," Altschul said. "We also urge Congress to recognize the interstate nature of location-based services and the mobility of wireless users so they take a national approach."

The EU's E-Privacy Directive is available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML>

The Article 29 Working Party's Opinion on the Use of Location Data is available at http://www.dataprotection.gov.sk/buxus/docs/wp115_en.pdf?buxus=c42c7261a54a802c63a0d1d276c7ed59

The Wireless and Communications Public Safety Act of 1999 is available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ081.106.pdf

EPIC's statement to the House Energy and Commerce Committee is available at http://epic.org/events/Locational_Data_Stmt.pdf

CTIA--The Wireless Association's "Best Practices and Guidelines for Location-Based Services" is available at http://files.ctia.org/pdf/CTIA_LBS_BestPracticesandGuidelines_04_08.pdf

More information on the European Union's November 2009 Amendments to the E-Privacy Directive is available at <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/1812&format=HTML&aged=0&language=EN&guiLanguage=en>

Copyright 2010, The Bureau of National Affairs, Inc.