Privacy in an Interconnected World

By Andrew B. Serwin, M. Leeann Habte, and Jerry D. Brown

The ubiquitous use of mobile devices, the Internet, wireless access, and the current developments in cloud computing have created new risks to the privacy of both business and personal information. Whereas technology is making rapid advances, the legal framework for the regulation of information that is stored or transferred using these devices is still in its infancy.

GPS and Cell Site Surveillance

Global positioning system (GPS) receivers are commonly used in cars and cell phones to provide location and directional assistance. These receivers can determine latitude, longitude, altitude, direction, and speed by receiving and processing location information from the transmissions of the four nearest orbiting GPS satellites. Increasingly, state and federal law enforcement officials are finding their own applications for GPS technology—specifically, to obtain evidence in criminal investigations. These officials have also begun obtaining evidence from tracking an individual's cell phone use. Historical cell site location information (which carriers typically keep for about 18 months) identifies the cell tower to which a customer was connected at the beginning of a call and at the end of the call. Unlike GPS data, cell site data can track a cell phone user's location while inside a residence.

GPS, cell sites, and the Fourth Amendment. Recent court cases addressing the challenges posed by GPS and cell site location information have forced a reevaluation of society's reasonable privacy expectations, and their treatment under the Fourth Amendment. Traditionally, the Fourth Amendment has protected information not previously disclosed to the public or third parties and particularly has applied to searches of a person's residence. GPS and cell phone

Andrew B. Serwin is a partner in the San Diego, California, office of Foley & Lardner LLP; he may be reached at **aserwin@foley.com.** ***M. Leeann Habte is an associate in the Los Angeles, California, branch of Foley & Lardner LLP; she may be reached at*** **lhabte@foley.com.** ***Jerry D. Brown is an associate at the Chicago, Illinois, office of Foley & Lardner LLP; he may be reached at*** **jbrown@foley.com.**

Published in GP Solo, Volume 28, Number 4, June 2011 © 2011 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

GPS and cell site data may implicate individual rights under the First Amendment.

technology have altered this understanding of privacy. Because they both raise the issue of surveillance of persons while in public, yet allow for almost continual observation that yields significant personal and intimate information about persons, some courts now recognize a Fourth Amendment privacy interest in being free from such continual unconsented electronic surveillance.

Moreover, GPS and cell site data also may implicate individual rights under the First Amendment. In *NAACP v. Alabama*, 357 U.S. 449 (1958), the U.S. Supreme Court held that a court could not compel the NAACP to produce its membership list because the First Amendment protects "freedom to associate and privacy in one's associations." The Court further stated that "[i]mmunity from state scrutiny of petitioner's membership lists is here so related to the right of petitioner's members to pursue their lawful private interests privately and to associate freely with others in doing so as to come within the protection of the Fourteenth Amendment" and, further, that the state's collection of the names of the NAACP's membership "would likely interfere with the free association of its members, so the state's interest in obtaining the records was superseded by the constitutional rights of the petitioners." Similarly, GPS and cell site tracking can reveal a person's religious or political affiliations or visits to medical professionals. This information may be just as revealing and intrusive as the membership list requested in *NAACP v. Alabama*.

Because GPS and cell site technologies facilitate and enable widespread unconsented and continuous surveillance of a person's public activity in ways that were previously technologically and logistically unfeasible, society's understanding and expectations of privacy must necessarily change.

GPS surveillance cases. Courts, both state and federal, have been split on whether a person has a Fourth Amendment privacy interest in GPS tracking data. A majority of federal courts have ruled that because such data concerns a person's movements in public, there is no Fourth Amendment right (and thus no need for law enforcement officials to secure a search warrant before beginning surveillance). Notably, however, in the case of *U.S. v. Maynard,* 615 F.3d 544 (D.C. Cir., 2010), the D.C. Court of Appeals ruled that the warrantless use by police of a GPS device attached to a person's vehicle to track his movements 24 hours a day for 28 days defeated his reasonable expectation of privacy in his movements over the course of a month, and was therefore a "search" under the Fourth Amendment. The *Maynard* court reasoned that although the GPS tracker was attached to the defendant's vehicle, the totality of a person's movements over the course of a month was neither actually or constructively disclosed to the public, and the prolonged GPS monitoring revealed an intimate picture of the person's life. In recognizing a Fourth Amendment interest in GPS tracking data, the *Maynard* court emphasized the information that can be inferred from the patterns in the collection of location data over the question of whether a person's location at a specific time was willingly disclosed to the public. The U.S. Supreme Court has yet to address this issue.

Cell site surveillance cases. Federal courts have generally approved government requests for warrantless unconsented access to a customer's cell site data under the Stored Communications Act (SCA), generally on the grounds that the data is in the possession of a third party and is therefore not protected by the Fourth Amendment. The SCA imposes a "less-than-probable cause standard," which is lower that the standard required for the Fourth Amendment. However, following the reasoning of *Maynard,* Magistrate Judge James Orenstein, in a denial of a government request for cell site data, held last year in *In re Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information*, 736 F. Supp. 2d 578, 2010 WL 3463132, at *3–14 (E.D.N.Y. Aug. 27, 2010), that when the government seeks access to historical cell site records for an extended period, it must satisfy the requirements for a warrant under the Fourth Amendment. For shorter periods such as three to 12 days,

Published in GP Solo, Volume 28, Number 4, June 2011 © 2011 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

however, a search warrant may not be necessary. Magistrate Orenstein's denial was reversed on November 29, 2010, by District Court Judge Roslynn Mauskopf. See also *In re Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information,* No. 10-MC-0897 (JO), 2010 WL 5437209, at *2–3 (E.D.N.Y. Dec. 23, 2010) and *In re U.S. for Historical Cell Site Data,* Nos. H–10–998M, H–10–990M, H–10–981M, 2010 WL 4286365 (S.D. Tex., Oct. 29, 2010).

Secondary uses of mobile data. The secondary use of data gathered from mobile devices has also come under fire in a number of recent class action suits. In December 2010 two separate groups of iPhone and iPad users filed lawsuits against Apple, Inc., in California District Court (*In re Freeman et al. v. Apple, Inc et al.*, and *In re Lalo v. Apple, Inc et al.*), and another was filed in early 2011 (*Chiu v. Apple, Inc*), alleging that certain software applications in mobile devices were passing personal user information to third-party advertisers without consent. The lawsuits allege that although Apple had agreed to amend its developer agreement to stop this from happening except for information directly necessary for the functionality of the applications, Apple had taken no meaningful action to this effect. In these suits, Apple has been charged with violation of the Stored Communication Act, the Computer Fraud and Abuse Act, and various California laws, as well as with common law invasion of privacy.

Cloud Computing

With the massive increases in bandwidth, wireless access, and mobile device use during the past decade, cloud computing is changing the way in which the Internet is used. Whether or not you are familiar with cloud computing, you are probably already using it. The "cloud" is a metaphor for the Internet. When combined with the word "computing," it refers to shared applications, virtual data centers, web-based applications, and managed computing services, all integrated through the Internet. Tax preparation, personal health records, e-mail, and social networking are examples of services that are commonly delivered through the cloud. For small legal practices and other businesses, cloud computing can offer low-cost access to sophisticated information-technology resources. Unfortunately, the law has not kept up with technological innovation, and the application of old law to new technology can be unpredictable. Therefore, lawyers should give careful consideration to the actual and potential privacy issues when using cloud computing services for their legal practices.

Existing law and cloud computing. Current laws that protect electronic communications may or may not apply to cloud computing or they may apply differently to different aspects of cloud computing. For example, the Fourth Amendment protections against unreasonable searches and seizures have not been clearly extended to the cloud. Under the rubric of "reasonable expectations of privacy," the Supreme Court has ruled that the Fourth Amendment protects the contents of telephone and other communications; however, these same protections are not afforded to transactional information disclosed to a third-party intermediary such as an accountant, bank, or telephone company. The implications of this third-party doctrine to the cloud computing environment, where information is turned over to cloud service providers for remote storage and other quasi-transactional purposes, are uncertain.

Although the Supreme Court has not yet addressed the application of Fourth Amendment constitutional protections to e-mail or other data in the cloud, a few lower courts have ruled on the issue. In the first ruling, *United States v. Warshak* 631 F.3d 266 (6th Cir. 2010), the Sixth Circuit found that consumers have a reasonable expectation of privacy in the content of e-mails stored on third-party servers. Although the exclusionary rule did not apply in this case, the Sixth Circuit held that an Internet service provider (ISP) that stores or sends e-mail is not a third party from whom electronic communication can be compelled without a warrant and is subject to the constitutional protections of the Fourth Amendment. The court's decision, however, did not

Unfortunately, the law has not kept up with technological innovation.

Published in GP Solo, Volume 28, Number 4, June 2011 © 2011 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

entirely bar warrantless searches. It noted that in some cases, such as where an ISP has a clearly stated policy of monitoring the contents of e-mails and actually does monitor them, a warrant would not be required. The court reasoned that in such instances, an informed user would not be able to maintain a reasonable expectation of privacy. As this case demonstrates, the privacy and confidentiality rights associated with data may vary depending on the terms of the service agreement and privacy policy established by the cloud provider. If a cloud provider maintains the right to change its terms and policies at will, the privacy risks would be heightened. Therefore, for a legal practice, understanding the terms of these cloud provider service agreements is key.

Regarding statutory law, the primary federal law is the Electronic Communications Privacy Act (ECPA), which protects wire, oral, and electronic communications in transit and stored communications. Title II of the ECPA, the Stored Communications Act (SCA), protects communications held in electronic storage, most notably messages stored on computers. Under the ECPA, stored communications are subject to protections, although weaker than those afforded by the Fourth Amendment. However, the application of the SCA to cloud computing is unclear. The Sixth Circuit in *Warshak* held that to the extent the SCA purports to permit the government to obtain such e-mails warrantlessly, the law is unconstitutional. Moreover, Section 2709 of the SCA, which allowed the Federal Bureau of Investigation to issue National Security Letters to ISPs ordering them to disclose records about their customers, was ruled unconstitutional in *John Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004). However, the decision was subsequently vacated by *Doe I v. Gonzales,* 449 F.3d 415 (2d.Cir. N.Y. 2006) after Section 2709 was amended by the U.S. Patriot Improvement and Reauthorization Act of 2005. Therefore, not only ECPA's applicability to data residing in the cloud, but also its constitutionality, is murky. Further, there is no clear regulatory framework that applies to the current technological environment.

Key privacy issues for cloud services. One important question about the cloud is whether privacy laws governing information prevent or limit the disclosure of certain records to third parties, including cloud computing providers. For example, health record privacy laws require a business associate agreement to legally share health information. Other privacy laws may prohibit personal information sharing by some corporate or institutional users. Professional secrecy obligations, such as those imposed on lawyers, might also inhibit the sharing of client information.

Even if the information can lawfully be shared, the location of information in the cloud impacts the privacy obligations of those who process or store the information. Information stored in the cloud actually resides on a physical machine owned by a particular company or person located in a specific country. Therefore, that data is subject to the laws of the country or state where the physical machine is located. If a cloud provider moves the user's information from one jurisdiction another, the provider's obligations for protection of the data could change. Further, data can be stored in multiple locations in the cloud. The places of business of the cloud provider, the location of the computer on which the information is stored, the location of the communication device that transmits the information between users and providers, and the location of the user are possible other locations where privacy obligations could be imposed on the cloud provider or user. Consequently, the data could be subject to multiple, differing privacy laws, which makes it difficult to accurately evaluate the confidentiality and privacy protections afforded data stored in the cloud.

Implications for legal practices. As discussed above, remote data storage may have adverse consequences for the legal protections of information. Information stored with a cloud computing service could be more susceptible to warrantless searches or seizures by government agencies or to access by private litigants. When information is legally privileged, the disclosure of that information with a cloud provider might be construed as a waiver of the attorney-client privilege. Whether the storage of a privileged communication or document with a cloud provider actually affects the privilege may depend in part on the terms under which the service is offered. If the cloud provider that stores the data disclaims the right to view or monitor the stored data, the argument for privilege may be stronger. However, if the cloud provider has the right to read, re-disclose, or transfer information entrusted to it, the argument for privilege would be weak.

In addition, a lawyer, who has a specific fiduciary or professional obligation to a client, must consider his or her ethical obligations. For example, the American Bar Association Model Rules of Professional Conduct establish a lawyer's duty to protect the confidentiality of information relating to the representation of a client. Rule 1.6 allows a lawyer to make disclosures without the client's consent that are implicitly authorized in order to carry out the representation, but it is arguable whether a lawyer's use of a cloud provider would qualify under this standard. Again, the cloud provider's terms of service might make a significant difference with respect to lawyer's ability to uphold his or her professional obligations. If the provider can use or disclose the client records, then the disclosure of information would likely breach this professional obligation.

Conclusion

Technological advances have made it possible to gather personal information (and draw inferences from it) and transmit and maintain it electronically more easily than was possible when the privacy laws (both statutory and case law) were developed. Courts and legislatures face the challenge of determining how the law will recognize and protect our privacy rights, and attorneys will have to regularly monitor the developments in this area. GPSOLO

Published in GP Solo, Volume 28, Number 4, June 2011 © 2011 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.