wiley

ARTICLE

ECPA Updates on the Table: A Harbinger of Litigation and Legislation

December 3, 2012

The law enforcement and civil liberties communities geared up for a markup on Thursday, November 29, 2012 of Sen. Patrick Leahy's (D-VT) proposals to update the Electronic Communications Privacy Act (ECPA). The updates focus on tightening and clarifying current restrictions on U.S. governmental entities that seek electronic information, including stored emails and "geolocation information." The legislation responds to perceptions of the civil liberty community, courts and some service providers that the existing legal framework for electronic surveillance and information-gathering is woefully obsolete in the face of 21st century technology. The proposals do not appear focused on the creation of additional or different restrictions on private entities' collection, use or voluntary disclosure of appropriate information to non-governmental entities. Though these amendments are not expected to pass in this Congressional term, they are expected to be debated again in the 2013-2014 term, and seem to be gaining bipartisan support.

ECPA Background

The ECPA, enacted in 1986, provides standards for law enforcement access to electronic communications and associated data. It struck a balance between privacy protections for emerging technologies and the needs of law enforcement. It imposes significant compliance burdens on a wide variety of private entities, some of which have become more vocal about their cooperation with law enforcement and their views on ECPA. While much of the law enforcement community is satisfied with existing authorities, many, including the Digital Due Process Coalition, argue that because technologies have advanced dramatically since 1986, the ECPA has been outpaced and is outmoded.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Privacy, Cyber & Data Governance
Public Policy
Telecom, Media & Technology

As one Court of Appeals observed almost a decade ago, "the [SCA] was written prior to the advent of the internet and the world wide web. As a result, the existing statutory framework is ill-suited to address modern forms of communication. . . . Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002). Several courts have remarked on the rapidly changing technology landscape, consumers' expectations of privacy in now-pervasive technologies and the seeming inadequacy of the existing legal regime. The legal framework "has not been amended to keep pace with changes in technology." *Crispin v. Christian Audigier, Inc.*, 717 F. Supp.2d 965, 972 (C.D.Cal. 2010).

As a result, various amendments to ECPA presently are under consideration. Two of Leahy's proposals stand out: Increased protection for stored email and clarification and increased protection for location information derived from mobile devices.

Stored Email Would Be Subject to Heightened Procedural Protections

Civil libertarians have long bemoaned the bright lines drawn in ECPA between "stored" email communications subject to lower privacy protections and those that receive more protection from government access. The Department of Justice (DOJ) has acknowledged that many have concerns about ECPA's treatment of stored communications — in particular, the rule that the government may use lawful process short of a warrant to obtain the content of emails that are stored for more than 180 days. Civil libertarians and others argue that this distinction makes no sense in an era where users leave emails in long-term storage with service providers, and in which individuals and businesses increasingly are using cloud computing.

To address some of this confusion and concern, Leahy proposes that the government be required to obtain a search warrant based on probable cause in order to obtain email content from a third-party service provider. His plan eliminates the outdated "180-day" rule that calls for different legal standards for the government to obtain email content depending upon the age of the emails in question. The government must notify an individual whose electronic communication has been disclosed, and provide that individual with a copy of the search warrant used to obtain the information within 10 business days. To address concerns that notice could compromise sensitive law enforcement investigations, however, Leahy's proposal provides that the government can seek a court order to delay notifying an individual for up to 180 days.

Government Entities Would Have to Meet New Requirements to Obtain "Geological Information"

Features that generate and rely on location information are built into numerous mobile devices and applications, which consumers use and enjoy. Mobile location technology is also the basis for several public safety initiatives, like the Commercial Mobile Alert System, which relies on device location and "geographic targeting" to "ensure that all Americans have the capability to receive timely and accurate" emergency alerts "irrespective of what communications technologies they use." 23 F.C.C.R. 6144, 6146 (2008). These advances generate information that is also of significant value to law enforcement.

Courts have been grappling with the legal status of location information derived from mobile devices. As the DOJ explained in 2011 to Congress, "[t]he appropriate legal standard for obtaining prospective cell-site information is not entirely uniform across the country. Judges in many districts issue prospective orders for cell-site information under the combined authority of a pen/trap order under the Pen Register statute and a court order" but "[s]tarting in 2005," some judges began concluding that "the only option for compelled ongoing production of cell location information is a search warrant based on probable cause." April 6, 2011, Written Testimony of James Baker, Associate Deputy Attorney General (ADAG), before the Committee on the Judiciary, U.S. Senate. These conflicting interpretations "have created uncertainty regarding the proper standard for compelled disclosure of cell-site information, and some courts' requirement of probable cause has hampered the government's ability to obtain important information in investigations of serious crimes." *Id.* Historical location information is relatively easy to obtain from service providers.

This uncertainty will draw U.S. Supreme Court attention. The Supreme Court recently decided a GPS location case, *United States v. Jones*, which did not involve information from a service provider but grew out of law enforcement's surreptitious physical attachment of a GPS tracking device to a suspect's car. Because the police did not abide the terms of the warrant authorizing the attachment, the defendant made a Fourth Amendment challenge to the use against him of the information gathered. The Supreme Court concluded that that a warrant was required. Associate Justice Antonin Scalia wrote, "[i]t is beyond dispute that a vehicle is an 'effect' as that term is used in the [Fourth] Amendment. We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search'" for which a valid warrant was required.

Jones was the most high profile of several cases percolating in the federal courts concerning location information, but did not address broader questions about individuals' Fourth Amendment interests in mobile location information from cell phones. Courts across the country have been struggling to categorize location information and determine the proper legal predicate for government access to it. A recent Sixth Circuit decision illustrates the sort of questions courts confront.

In *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012), police obtained a warrant to intercept calls, and "an order from a federal magistrate judge ... authorizing the phone company to release subscriber information, cell site information, GPS real-time location, and 'ping' data" for the mobile phone the suspect was thought to be using. Agents "pinged" the phone to get its location and used that information to secure additional, similar orders for other phones in use. The defendant claimed that the use of the GPS location information emitted from his cell phone was a warrantless search that violated the Fourth Amendment. The Sixth Circuit robustly disagreed. "There is no Fourth Amendment violation because Skinner did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone." The court reasoned that "the recent nature of cell phone location technology does not change" the common-sense notion that "[t]he law cannot be that a criminal is entitled to rely on the expected untrackability of his tools. ... If it did, then technology would help criminals but not the police." Lest the reader think this conclusion was limited to criminals, the court clarified: "On the contrary, an innocent actor would similarly lack a reasonable expectation of privacy in the inherent external locatability of a tool that he or she bought." *Id.* at n.1. *Skinner*

drew a great deal of commentary both about Fourth Amendment principles and technology questions implicit in the opinion. For example, GPS location information and cell-site location information are different, though courts often elide the distinction when addressing location information. A petition for rehearing *en banc* was denied on September 26, 2012 and the case is a good candidate for Supreme Court review.

This sort of litigation will continue until the Supreme Court or Congress resolves uncertainty about the legal status of location information. Leahy proposes amending ECPA to include a new category of "geolocation information" which would have demanding requirements for access by governmental entities. Government entities would be generally prohibited from accessing geolocation information without a warrant or court order under the Foreign Intelligence Surveillance Act (FISA), except to respond to an emergency. Under Leahy's proposal, a communications provider could be required to grant government access to a user's contemporaneous or prospective geolocation information if presented with a warrant or in order to respond to a user's call for emergency services. A communications provider could be required to grant government access to historical geolocation information if presented with a warrant, a court order under FISA, or when the government has the subscriber's consent.

On their face, these proposals only address government access to geolocation information. While some commentators are uneasy about private entities' use and exploitation of location information, these proposals do not appear aimed at restricting private use of location information. That said, the immunity provisions contained in Leahy's proposal protect entities from liability for providing information to "governmental entities" pursuant to the statute. It does not rule out the possibility of creative lawsuits flowing from sharing such information with others.

Current State of Play

Debate over ECPA reform has been percolating for a while. Key players include the White House, DOJ, state and local law enforcement agencies, telecommunications companies, Internet Service Providers, makers and sellers of mobile telephone applications, civil liberty advocates, and privacy advocates.

At the Senate Judiciary Committee Mark-Up held November 29, the committee voted in favor of Leahy's heightened procedural protection for stored email communications and geolocation information, by voice vote. Before approving the bill, the panel voted 6-11 to reject an amendment by Sen. Chuck Grassley (R-IA) that would exempt the measure's warrant requirement for investigations of crimes involving child abduction. And to address certain sensitive investigations, an amendment to the proposal from Sen. John Cornyn (R-TX) and Sen. Mike Lee (R-UT), modified the provisions requiring notice to persons whose data is accessed. The modification reduced the period in which access without notice would be permissible from 180 days to 90 days for governmental entities that are not law enforcement agencies.

Despite committee approval, chances for ultimate passage are slim in this Congress. However, the committee's blessing of these changes may set the terms of debate for next year.

Conclusion

Passage of these amendments to ECPA this year seems remote, but chatter will continue as courts and those directly impacted continue to grapple with uncertainty. The increase in attention to these proposals, coupled with support across a broad swath of interested parties, make it more likely that Congress will act in 2013. The stage has been set: Some service providers may continue to seek clarity in the law, while civil libertarians will seek additional privacy protections. Law enforcement will aim to protect its ability to efficiently and creatively investigate and prosecute crime. In 2013, this process may come to a close with enactment of significant amendments to ECPA.