wiley

ARTICLE

Internet Of Things Cos. Must Prepare For Law Enforcement

Law360
August 16, 2018

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Stephen J. Obermeier
Partner
202.719.7465
sobermeier@wiley.law

Vesna K. Harasic-Yaksic
Partner
202.719.4506
vharasic-yaksic@wiley.law

Practice Areas

Internet of Things

Privacy, Cyber & Data Governance

United States law enforcement is changing investigative tactics. Vast amounts of personal and business data can be collected and stored by companies through internet of things devices, and the government has noticed. As the Berkman Center for Internet and Society at Harvard predicted in the context of concerns about "going dark" due to encryption of traditional telephonic communications and handsets:

Networked sensors and the Internet of Things are projected to grow substantially, and this has the potential to drastically change surveillance. The still images, video, and audio captured by these devices may enable real-time intercept and recording with after-the-fact access. Thus an inability to monitor an encrypted channel could be mitigated by the ability to monitor from afar a person through a different channel.[1] We anticipate that law enforcement will follow

the data, causing a major shift for companies that previously had minimal contact with criminal investigators. This article provides an overview of traditional investigative techniques and explores some of the questions companies will need to resolve as their products and services rapidly go online.

Paradigm Shift in Criminal Investigations

From corporate fraud to murder, law enforcement has looked for decades to internet service providers and traditional telecommunications companies as a source of evidence. Increasingly, law enforcement is looking beyond these traditional sources of electronic data to more creative ways to build a case. For example, in a recent case, law enforcement's collection of information from a cardiac pacemaker played a key role in charging an individual with both arson and insurance fraud.[2] In that case, the defendant called 911 soon after his house caught on fire, explaining that he ran around his house collecting his belongings before escaping through a window. Law enforcement successfully obtained a warrant for his pacemaker, which undermined his story based on information related to his heart rate during the incident. Similarly, in Connecticut, a murder victim's Fitbit recently was used to establish the falsity of her murderer's alibi based on the distance she had traveled before her death.[3]

While these cases are currently on the cutting edge, in the coming years, these requests will become routine. Depending on how an IoT device is configured and the type of data it collects, the evidence held by IoT companies may be useful or even decisive in legal disputes and criminal investigations. As such, we anticipate that IoT device companies increasingly will receive inquiries and court orders from law enforcement.

The World of Electronic Data Collection: Wiretap Orders, Search Warrants, 2703(d) Orders and Subpoenas

Law enforcement uses a wide range of investigative tools, frequently under the Wiretap Act and Electronic Communications Privacy Act, when obtaining electronic evidence in criminal investigations.

Law enforcement can obtain real-time communications, including emails, chats and web browsing, using a wiretap.[4] Noncontent information, like IP addresses and email headers, can be obtained in real-time using a pen/trap order.[5] These "surveillance" tools are often very powerful, but also more difficult to obtain, requiring that law enforcement meet rigid requirements in addition to showing probable cause for the evidence.

Historical content information can also be obtained pursuant to a search warrant supported by probable cause under ECPA.[6] These are regularly used to obtain the contents of social media accounts, emails or, in limited circumstances, the contents of a website.[7] Noncontent information, like subscriber information and transactional logs, commonly IP addresses, are available under a court order under 18 U.S.C. 2703(d). A 2703 (d) order merely requires a showing that the records sought are relevant and material to an ongoing criminal

investigation. Finally, law enforcement can obtain subscriber information using only a subpoena issued by an authorized official in conjunction with an administrative proceeding, grand jury investigation or trial.

IoT companies should expect this legal regime to apply to law enforcement requests for electronic information collected by IoT devices as well.

What Should IoT Companies Be Thinking About?

The traditional ISPs and telecommunications companies that receive these requests often have robust compliance departments to handle — and when necessary, litigate — requests from law enforcement. Transparency reports indicate that ISPs and carriers receive hundreds of thousands of requests annually.[8]

We anticipate that IoT device companies that are not currently accustomed to responding to law enforcement will face a variety of issues as they stand up compliance policies and procedures. We have identified the following areas that forward thinking IoT device companies should start considering as they begin to receive requests for user data:

What is your philosophy on law enforcement assistance and compliance?

Some companies are by-the-book; they won't provide the government with any information or assistance unless served with a proper court order. Other companies are more willing to work with law enforcement to shape compliant requests. At the other end of the spectrum, some companies are openly hostile.

Whatever approach a company takes with respect to law enforcement, it can affect both the public and the government's perception of the company. Telecommunications companies faced lengthy and burdensome litigation after a post 9/11 surveillance program was disclosed in the press.[9] More recently, after Edward Snowden's theft and leak of information about NSA surveillance, parts of the U.S. tech sector faced scrutiny and some backlash[10] from domestic and overseas customers. The leaks also spurred international regulatory responses; Russia enacted data localization laws, and China blocked some U.S. companies from operating within its borders. Arguably, the European Union's push for broader extraterritorial data privacy laws, like its General Data Protection Regulation, has been in part a reaction to U.S. law enforcement's interactions with technology companies.

On the flip side, federal, state and local governments across the United States have legitimate, often pressing needs for electronic data; they need the cooperation of the private sector to obtain critical data. A professional working relationship with government may be more than good corporate citizenship; it can be helpful to companies who need government assistance, for example, when they are the victims of cyber attacks or computer hacking.

Based on past experience of the ISP and telecommunications sector, IoT device companies can expect to face

competing pressures with respect to interacting with law enforcement, which should inform technical, legal and even marketing decisions.

How will you approach consent?

Traditional notions of consent may not fit in an IoT world. For many ISPs and telecommunications companies, the terms of service and user-facing privacy policy govern much of the relationship between a company and its users, including explaining under what circumstances data will be provided to law enforcement and how disputes could be resolved.

Many IoT devices will be collecting significant amounts of data generated by or related to individuals who may not be in privity with companies, making consent and dispute resolution more complex. Without a privacy policy or terms of service to rely on, the legal ability of a company to provide data to law enforcement may be more complicated, especially as additional states enact specific privacy laws.[11] These complexities may generate customer relations issues and litigation.

Where will you store your data?

Companies face increasingly fraught choices about where they will hold their data; as we move toward more distributed networks and cloud storage, these questions become even more complex. For example, in the United States, the Cloud Act, which was passed in March of 2018, provides that domestic law enforcement has authorization to obtain electronic data that is "within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."[12] Although the Cloud Act helps to clarify the extent of U.S. authority, the reality is that global companies are likely to face inconsistent orders from different countries and may face situations where refusal to comply with a foreign law enforcement request may directly impact the ability to do business in a country.

IoT device companies may face different regulatory regimes depending on where they store user data; their choices can affect law enforcement access and potentially make data more accessible to non-U.S. governments.[13]

How do U.S. surveillance laws affect you? ECPA and CALEA

The relationship between law enforcement and telecommunications companies and ISPs are largely governed by two statutes: (1) the Communications Assistance for Law Enforcement Act and (2) ECPA. CALEA generally applies to a "telecommunications carrier" that is a "common carrier for hire."[14] Although most IoT devices will not be regulated by CALEA, those that do will be required to implement the ability to conduct live surveillance prior to receiving a wiretap or pen/trap order, which can be a substantial undertaking.

On the other hand, ECPA creates several restrictions for "electronic communications services" and "remote

computing services," including prohibiting the disclosure of subscriber information and content to the government without proper legal process.[15] Applying ECPA's antiquated terms to IoT devices will likely present challenges and edge cases, which will not only affect how companies interact with their users and the government, but can also create a risk of civil litigation if information is disclosed in alleged violation of ECPA.

How will you apply Fourth Amendment principles to unconventional categories of data?

Several recent U.S. Supreme Court rulings have expanded the Fourth Amendment to require a warrant before law enforcement obtains certain electronic information.[16]

In its most recent decision on data privacy, Carpenter v. United States, the Supreme Court concluded that the government must obtain a search warrant when seeking historical cell tower records providing a detailed and comprehensive history of a user's movements. This decision — which rejected the U.S. Department of Justice's long-standing practice of collecting cell-site location information via an order pursuant to 18 U.S.C. § 2703(d) — acknowledged that technology is a necessity of modern life and that certain categories of data have the power to reveal a wealth of personal information.[17]

Although Carpenter dealt with a specific category of data — that is, location information derived from cell tower records — it is unclear how the Supreme Court's expansion of Fourth Amendment privacy protections will impact other categories of data. Indeed, many IoT devices collect data that do not fit squarely within our legal framework. As such, the Supreme Court's recent expansion will undoubtedly spark difficult debates between law enforcement and IoT device companies about the process required for data that falls within "gray areas" of the law. These disputes will carry risks and opportunities for companies to distinguish themselves as either supporters of law enforcement or advocates for individual privacy.

How will you approach encryption? Since the 1990s, law enforcement and privacy advocates have debated the need and appropriateness of requiring companies to decrypt data in criminal investigations. At present, the government generally cannot force ISPs and telecommunications companies to decrypt users' information, and technology companies have largely resisted the government's push for backdoors to encryption.[18] This fight most recently played out in the legal battles between Apple and the FBI over decrypting iPhones.[19]

IoT device companies will face many of the same encryption questions that ISPs face and will likely become part of the debate over whether Congress should force a backdoor for encryption.

How will you handle discovery in civil matters? It is worth noting that law enforcement will not be the only party looking to mine electronic data for evidence. Such data can also be requested by a party to a civil proceeding pursuant to subpoena under Federal Rule of Civil Procedure 45 (or civil discovery if an IoT company is a party to a civil suit).

Under ECPA, civil litigators do not have the same tools as law enforcement and are generally prohibited from

obtaining the content of communications with a third-party subpoena.[20] However, some data — such as phone records — are easily collected and not protected under ECPA.

Rule 45 provides in part that "[t]he person responding [to a third-party civil subpoena] need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost." IoT device companies may be able to use this limitation to prohibit widespread fishing exhibitions of every IoT device connected with litigation. However, some data certainly will be discoverable in civil matters. As a result, IoT device companies may decide to adopt a general policy of compliance, finding that the burden of litigating motions to quash is not worth the time and expense.

Conclusion

As the IoT device market develops, companies can expect their relationships with consumers, the public and law enforcement to become more complicated, and, at times, contentious. Holders of data as well as those that control IoT devices and services that can be used in surveillance should work to proactively manage those relationships now, before they receive a subpoena.

Specifically, maturing companies in the IoT space should ask themselves the following questions:

- What data about consumers and the public are you holding, and where are you holding that data?
- Can you explain to the government what you can provide and what process you demand?
- Do you have policies and procedures for responding to government requests for such data?
- Are you prepared to enforce your terms of service and user-facing privacy policy in order to avoid litigation and regulatory oversight?
- Will you treat non-U.S. governments differently?
- What do you want to tell consumers about how you will respond to law enforcement?
- Will you engage in transparency efforts with the public, including notifying individuals if law enforcement requests their data?

- Are you prepared to comply with gag orders under 18 U.S.C. 2705 and sealing orders preventing you from publicly disclosing a law enforcement request?

  - How aggressive will you be in litigation with the government, as opposed to negotiating a resolution?

- How will you respond to requests for data in civil proceedings?

IoT companies that are proactive in this space and develop a coherent strategy should be able to avoid many of the pitfalls that are sure to come as law enforcement changes the way it investigates cases.

---

[1] Don't Panic. Making Progress on the Going Dark Debate (2016)

[2] See Wired, Your Own Pacemaker Can Testify Against You in Court, July 29, 2017 (available at: https://www.wired.com/story/your-own-pacemaker-can-now-testify-against-you-in-court/).

[3] See New York Times, In Connecticut Murder Case, Fitbit is a Silent Witness, April 27, 2017 (available at: https://www.nytimes.com/2017/04/27/nyregion/in-connecticut-murder-case-a-fitbit-is-a-silent-witness.html).

[4] See 18 U.S.C. § 2510 et seq.

[5] See 18 U.S.C. § 3123 et seq.

[6] See 18 U.S.C. § 2703(b).

[7] Lauren Rosenblatt, Judge approves limited search warrant for data on anti-Trump protesters, L.A. Times Aug. 24, 2017, http://www.latimes.com/politics/la-na-pol-justice-department-dreamhost-20170824-story.html#.

[8] See, e.g., Transparency Report, Verizon, http://www.verizon.com/about/portal/transparency-report/us-report/ (disclosing that Verizon received roughly 271,000 law enforcement requests in 2017); Transparency Report, AT&T, http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html (describing national security requests and routine LEA requests); Transparency Report for 2016, T-Mobile US, Inc., https://www.t-mobile.com/content/dam/t-mobile/corporate/media-library/public/documents/TransparencyReport2016.pdf; Transparency Report, Google, https://transparencyreport.google.com/user-data/overview.

[9] See Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006) (claiming that AT&T's alleged involvement in the NSA's surveillance program violated the Electronic Communications Privacy Act). It took several years of litigation and an act of Congress to terminate this litigation, which shows the risk that companies take when they assist the United States.

[10] See Daniel Castro & Alan McQuinn, Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness, Information Technology & Innovation Foundation, June 2015, http://www2.itif.org/2015-beyond-usa-freedom-act.pdf?_ga=1.114044933.369159037.1433787396) (impact "likely far exceed[s]" loss of $35 billion).

[11] See, e.g., Illinois Biometric Information Privacy Act, 740 ILCS 14 (regulating collection and use of biometric information).

[12] See 18 U.S.C. 2713.

[13] Some countries require data localization as a prerequisite to getting licenses or otherwise doing business in the country. Matthew Newton & Julia Summers, Russian Data Localization Laws: Enriching "Security" & the Economy, Henry M. Jackson School of International Studies, Feb 2018, https://jsis.washington.edu/news/russian-data-localization-enriching-security-economy/.

[14] See 47 U.S.C. 1001(8).

[15] See 18 U.S.C. 2702(a); Quan v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008) ("Wireless communications provider ... violated [ECPA] when it knowingly released archived transcripts of police officers' text messages to city at city's request ... .").

[16] See, e.g., United States v. Jones, 565 U.S. 400 (2012) (finding that the installation of a GPS tracking device

on a vehicle and using the device to monitor the vehicle's movements for several days constituted a search under the Fourth Amendment); Riley v. California, 134 S.Ct. 2473 (2014) (Fourth Amendment requires a warrant for search of cell phone incident to arrest based in part volume and scope of private information stored on cell phones.).

[17] See United States v. Jones, 132 S.Ct. 945 (2012) (J. Alito, concurring) ("Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. ... A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups — and not just one such fact about a person, but all such facts.").

[18] See 47 U.S.C. § 1002(b)(3) (A "telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.").

[19] See In re Order Requiring Apple to Assist in Execution of a Search Warrant, 149 F.Supp.3d 341, 354 (E.D. N.Y. 2016) (denying government's request under the All Writs Act to force Apple to bypass iPhone security features); Government's Motion to Compel in San Bernardino investigation (available at: https://www.justice.gov/usao-cdca/file/826836/download).

[20] See, e.g., Crispin v. Christian Audigier Inc., 717 F.Supp.2d 965 (N.D. Cal. 2010) (quashing subpoenas to Facebook and MySpace); Viacom International Inc. v. Youtube Inc., 253 F.R.D. 256, 264 (S.D.N.Y. 2008) (holding that ECPA prohibits disclosure of information pursuant to a civil subpoena because the Act "contains no exception for disclosure of such communications pursuant to civil discovery requests"); O'Grady v. Superior Court, 139 Cal. App. 4th 1423, 44 Cal. Rptr. 3d 72 (2006) (emphasizing the substantial burden and expense that would be imposed on internet service providers if they were required to respond to every civil discovery subpoena issued in a civil lawsuit).