Carpenter and Everything After: The Supreme Court Nudges the Fourth Amendment into the Information Age

By Christopher C. Fonzone, Kate Heinzelman, and Michael R. Roberts

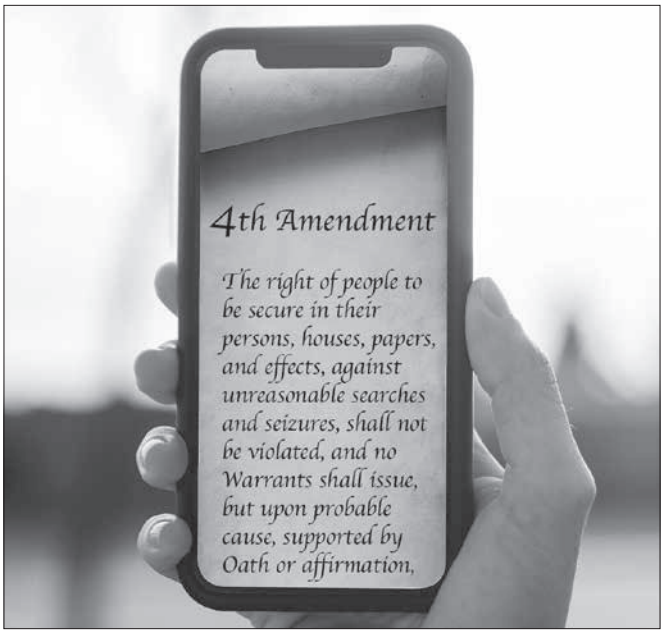
Every year, as the calendar turns to June, the legal community looks to the Supreme Court. Eager to get to the Term's end, the Justices rush to complete all of the outstanding opinions. Since the most difficult and important cases usually take the longest to work out, they are typically the stragglers. June is thus the time when the "blockbuster" opinions are issued—the cases that law professors analyze in their tenure pieces and that law school students study, quite possibly for years to come.

In June 2018, consistent with this history, the legal community awaited the Court's decision in *Carpenter v. United States*,[1] a case that considered whether the Fourth Amendment protects an individual's historical cell-site locational information ("CSLI") even if the information is in the possession of a cellular service provider. Heading into *Carpenter*, the so-called "third-party doctrine," established by the Court over 40 years ago, was understood to stand for the principle that the Fourth Amendment generally did not protect information, such as phone or banking records, voluntarily provided to others. Yet digitization and technological advances had increasingly placed the doctrine under pressure, as an increasing amount of potentially revealing information is now in the hands of third parties. Scholars, advocates, and commentators thus wondered what the Court would do in its direct encounter with what is likely one of the foundational Fourth Amendment issues of our time: Would it hold that the Amendment offers no protection to the digital tracks that are a necessary byproduct of the Information Age? Or would it reverse a doctrine that law enforcement officials have relied on for two generations?

Fonzone

Heinzelman

Roberts



In fact, the Court appeared to do neither. By a vote of five to four, the Court held that an individual has a "reasonable expectation of privacy" in historical CSLI and that the Fourth Amendment therefore does protect such data even if the information is in the possession of a wireless carrier. This prompted commentators to almost immediately label *Carpenter* a landmark search and seizure decision. At the same time, however, the Court went out of its way to emphasize that its opinion was "narrow" and marked no dramatic shift in Fourth Amendment

Christopher C. Fonzone (cfonzone@sidley.com), formerly deputy assistant and deputy counsel to President Obama and the legal adviser to the National Security Council, is a partner in Sidley Austin LLP's Privacy and Cybersecurity practice. Kate Heinzelman (kheinzelman@sidley.com), formerly deputy general counsel at the Department of Health & Human Services and associate counsel to President Obama, is a counsel in the firm's Healthcare and Privacy & Cybersecurity practices. Michael R. Roberts (mrroberts@sidley.com), formerly a White House intern in the Office of the Counsel to Vice President Biden, is an associate in the firm's Privacy and Cybersecurity group.

jurisprudence. In short, *Carpenter* is an opinion with potentially dramatic implications but explicit statements that caution against reading too much into it.

So what should businesses make of *Carpenter* given this apparent discrepancy between the critical commentary and the Court's statements? The Government can, of course, request customer or other third-party information at any time, and businesses must understand how to respond. In anticipation of such requests, this article provides a quick primer for infrastructure companies on what *Carpenter* said and what, as a practical matter, it might mean for them.

Carpenter: What Did It Say?

The relevant facts underlying *Carpenter* are straightforward: a suspect confessed to a string of robberies and, based on the information he provided and further information obtained from his call records, the Federal Bureau of Investigation ("FBI") identified phone numbers of interest, including Timothy Carpenter's. The FBI subsequently sought and obtained two court orders under the Stored Communications Act ("SCA") requiring Carpenter's wireless carriers to provide CSLI from around the time of the robberies. One order sought 152 days of CSLI from one provider, the other seven days from another. Importantly, the SCA allowed the FBI to secure these orders based on a showing, not of probable cause but, rather, of "specific and articulable facts" that "there are reasonable grounds to believe" the records sought "are relevant and material to an ongoing criminal investigation."[2] Carpenter subsequently sought to suppress the CSLI on the grounds that the Fourth Amendment required a warrant backed by probable cause to compel its production.

The Sixth Circuit rejected Carpenter's claim on the ground that the Fourth Amendment did not protect the CSLI because Carpenter had provided it to a third-party—his wireless carrier.[3] However, the Supreme Court, in a 5–4 decision, reversed. Three key pillars of the Court's reasoning are notable: (1) Carpenter had a "reasonable expectation of privacy" in the CSLI and the Fourth Amendment thus protected it; (2) a third party holding the information did not deprive Carpenter of his "reasonable expectation"; and (3) the Government could only compel the production of the CSLI with a probable cause warrant.

"Reasonable Expectation of Privacy"

The Court grounded its analysis of Carpenter's claim in its landmark *Katz* decision. *Katz* famously stated that a warrant is generally required when an individual "seeks to preserve something as private" and the expectation of privacy is "one that society is prepared to recognize as reasonable."[4] The Court acknowledged that there is no definitive approach for applying *Katz*'s test but identified several aspects of the historical CSLI at issue that made Carpenter's expectation of privacy in the information both subjectively and objectively reasonable.[5]

Its "All-Encompassing" Nature

The Court emphasized that people "carry cell phones with them all the time," such that tracking the phone's location provides an "an all-encompassing record of the holder's whereabouts."[6] Moreover, because wireless carriers often retain CSLI for five years, the Government can thus obtain "retrospective" CSLI—well over 100 days' worth in Carpenter's case.[7] This means that law enforcement efforts to reconstruct the past are no longer limited by "a dearth of records and the frailties of recollection"; rather, the Court emphasized, "[w]hoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years."[8]

Its Invasiveness

CSLI is not only abundant, the Court reasoned, but it also "provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations."[9] Drawing on its own precedents, the Court emphasized that these associations "hold for many Americans the privacies of life."[10]

The Hidden Manner in which It Is Collected

The Court also emphasized that CSLI tracking is largely hidden. As the Court put it, allowing the Government access to Carpenter's CSLI without having to satisfy the Fourth Amendment's requirements contravenes "society's expectation" that "law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue [an individual's] every single movement . . . for a very long period."[11]

The Ease and Efficiency of Obtaining the Information

Finally, the Court emphasized that "cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools."[12] As commentators have noted, while this trait doesn't necessarily speak to Carpenter's expectation of privacy, it does recognize that new technologies like CSLI dispense with "friction as a source of privacy protection" and create a "difference in the power of surveillance [that] simply cannot be ignored."[13]

The Third-Party Doctrine

Importantly, in finding that Carpenter had a reasonable expectation of privacy, the Court also explicitly rejected the notion that the third-party doctrine resolved the case. The Court acknowledged that, in *United States v. Miller*,[14] it had held that an individual does not have a reasonable expectation of privacy in banking records voluntarily turned over to third parties, and that, in *Smith v. Maryland*,[15] it had reached a similar conclusion

with respect to dialed phone numbers. The Court, however, rejected the Government's argument that those cases controlled this one.

> The Government's position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years. . . . There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today.[16]

The Court highlighted another reason the "third-party doctrine" was unsuitable to the CSLI at issue in this case: users in no real sense voluntarily expose their CSLI to their wireless provider. As the Court emphasized, "cell phones and the services they provide are such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society" and, because a cell phone logs locational data merely "by dint of its operation," there is "no way" for users "to avoid leaving behind a trail of" CSLI.[17]

The Need for a Warrant

A final aspect of the Court's decision worth highlighting was its determination that the Government would generally be required to obtain a warrant before acquiring records like Carpenter's CSLI. The Court's logic was straightforward: because Carpenter had a reasonable expectation of privacy in his CSLI, the acquisition of Carpenter's CSLI was thus a search, and the Government therefore must "generally obtain a warrant supported by probable cause before acquiring such records."[18] In taking this position, the Court rejected Justice Alito's strongly worded dissent, which argued that:

> the Court ignores the basic distinction between an actual search (dispatching law enforcement officers to enter private premises and root through private papers and effects) and an order merely requiring a party to look through its own records and produce specified documents. The former, which intrudes on personal privacy far more deeply, requires probable cause; the latter does not. Treating an order to produce like an actual search, as today's decision does, is revolutionary.[19]

The Court, however, contested Justice Alito's reading of its precedents, finding that it had "never held"—as Justice Alito would have in *Carpenter*—"that the Government may subpoena third parties for records in which the suspect had a reasonable expectation of privacy."[20] A warrant was therefore generally required to acquire the historical CSLI at issue in this case, although there may be certain situations, such as exigent circumstances, where one is unnecessary.

And Everything After: What Does *Carpenter* Mean?

Carpenter is not the first recent case in which the Court has considered how the Fourth Amendment applies to new technologies. In 2012, *United States v. Jones*[21] presented the question of whether the FBI violated a suspect's Fourth Amendment rights by installing a GPS tracking device on his vehicle and remotely monitoring the vehicle for nearly a month. The Court held that the installation of the device was unconstitutional based on the Government's physical trespass of the suspect's vehicle, but, as *Carpenter* highlighted, five Justices also noted that the tracking itself would raise constitutional concerns.[22] Likewise, just two years later, in *Riley v. California*,[23] the Court confronted the question of whether the police could conduct a warrantless search of an arrestee's cell phone. Rejecting the idea that the warrant exception for searches incident to arrest applied, the Court recognized that the "immense storage capacity" of modern cell phones "implicate[s] privacy concerns far beyond those implicated by the search of" the sort of physical objects arrestees would have had on them at the time the doctrine was developed.[24]

Despite these prior cases, interest in *Carpenter* still ran unusually high, because, as noted at the outset, it squarely presented a foundational question about the Fourth Amendment in the Information Age: whether individuals' digital footprints are left unprotected because they are in the possession of third parties. As Justice Alito noted in his dissent, law enforcement and other government authorities can use the SCA, and a number of other statutes, to acquire a wide variety of records held by third parties without a warrant.[25] This point, in turn, means that the Court's holding in *Carpenter* that a warrant is required to access CSLI held by a wireless carrier could have dramatic implications for both information holders and Government investigators.

Which is likely why the Court went out of its way to present its *Carpenter* holding as a decidedly "narrow one":

> We do not express a view on matters not before us: real-time CSLI or "tower dumps" (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security.[26]

In short, the Court made a point of encouraging people not to read too much into its decision, leaving a potential divide between what the decision explicitly said and what a wide range of commentators think it meant.[27] To be sure, lower courts—and eventually the Supreme Court itself—will have to apply *Carpenter*'s reasoning to new scenarios, resolving some of this ambiguity and clarifying this developing area of law. But information holders—including infrastructure providers that often hold data concerning individuals—will necessarily be presented with the question of how to respond to law enforcement requests for such "third party" data before lower courts have fully fleshed out *Carpenter*'s implications. Recognizing that there are limits to what can be said at this point of doctrinal development, we provide some preliminary thoughts, informed by nearly a year of lower-court case law applying *Carpenter*, about how industry should be thinking about the case.

First, the most important takeaway from *Carpenter* is that merely because a third party provided or generated information in a company's possession does not *necessarily* mean that the individual has no Fourth Amendment interest in that information. In hindsight, this is perhaps unsurprising. At least since *Katz*, which concerned the contents of a phone call, the Court has recognized that an individual has a reasonable expectation of privacy in, and the Fourth Amendment therefore protects, certain forms of content that are being provided to a third party.[28] But, in the wake of the broad language used in the Court's opinions in *Smith* and *Miller,* the "third-party doctrine" was understood by many to be essentially a bright-line rule, particularly when it came to the sort of information at issue in *Carpenter—e.g.,* information that did not involve communication contents.[29] Thus, if *Carpenter* requires anything, it requires companies to, at the very least, consider whether any third-party information in their possession is constitutionally protected.

Second, in considering their third-party records, businesses should be cognizant of the fact that *Carpenter* strongly signals that the constitutional status of "conventional surveillance techniques and tools, such as security cameras" has not changed. This means that the "third-party doctrine" still governs what one commentator has called, "20th Century business records," *i.e.*, the bank and phone records at issue in *Smith* and *Miller* and business records like them.[30]

Third, even beyond the sorts of traditional records at issue in *Smith* and *Miller*, businesses should be cautious about assuming that third-party information they hold is constitutionally protected. *Carpenter* states that it is a "rare case" in which third-party records would receive constitutional protection,[31] and it explicitly reserves the question of whether information very similar to historical CSLI—real time CSLI and "tower dumps"—should be treated the same as third-party data. Indeed, the *Carpenter* decision goes so far as to suggest that fewer than seven days of historical CSLI, the minimum amount at issue in the case, could be treated differently.[32]

But *Carpenter* should not be taken to mean that all information created by modern technology except for more than seven days of historical CSLI is beyond the reach of the Fourth Amendment. Other forms of information may possess many, or all, of the attributes that the Court found important in *Carpenter*: an "all-encompassing" nature and the fact that it provides an "intimate window" into someone's life, that it was captured in a hidden manner, that it can provide vast quantities of information to law enforcement in an easy and efficient manner, and that it was not collected in a manner that can reasonably be understood as voluntary. It will be left to future cases to provide definitive guidance on how these traits apply to specific categories of information. In the interim, companies will have to do their best to assess the third-party information they possess against these attributes in order to decide whether access requires a warrant.

Lower courts, in fact, appear to be taking this approach. Certainly, the majority of the federal cases that have considered *Carpenter* have either confronted questions about whether the "good faith" exception to the warrant requirement demands suppressing CSLI acquired prior to the Court's *Carpenter* decision or they have simply applied the Court's explicit guidance not to disturb traditional investigative methods.[33] Nonetheless, a Seventh Circuit Court of Appeals decision suggests a potential approach to *Carpenter*, as well as the case's possible importance, and this lower court decision is particularly relevant to infrastructure providers.

In *Naperville Smart Meter Awareness v. City of Naperville* ("*Naperville Smart Meter*"),[34] a citizens' group sued the City of Naperville, arguing that digital smart meters that recorded electricity consumption at 15-minute intervals violated the citizens' Fourth Amendment rights. The City argued that the consumption readings were constitutionally unprotected third-party records. However, the Seventh Circuit roundly rejected the City's position and instead relied on factors the Court emphasized in *Carpenter*, in other words, the "constant" nature of the monitoring and that the information is not provided voluntarily. The Seventh Circuit stated:

> The third-party doctrine rests on the notion that an individual has a reduced expectation of privacy in information knowingly shared with another. But in this context, a choice to share data imposed by fiat is no choice at all. If a person does not—in any meaningful sense—voluntarily assume the risk of turning over a comprehensive dossier of physical movements by choosing to use a cell phone, it also goes that a home occupant does not assume the risk of near constant monitoring by choosing to have electricity in her home.[35]

While the Court found that the information was protected by the Fourth Amendment, it nevertheless found that the smart meter monitoring at issue survived Fourth Amendment scrutiny on the grounds that the monitoring was reasonable.

Thus, the Seventh Circuit's decision in *Naperville Smart Meter* demonstrates a *fourth* key point that companies should consider: even if the Fourth Amendment protects third-party information, the Government may still be able to access the information without a warrant. Because the consumption monitoring at issue in *Naperville Smart Meter* was not part of a criminal investigation, the Seventh Circuit simply assessed whether the monitoring was reasonable under the Fourth Amendment. The Seventh Circuit noted that warrantless searches are presumed unreasonable but found that the compliance monitoring overcame that presumption.

> Smart meters allow utilities to reduce costs, provide cheaper power to consumers, encourage energy efficiency, and increase grid stability. We hold that these interests render the city's search reasonable, where the search is unrelated to law enforcement, is minimally invasive, and presents little risk of corollary criminal consequences.[36]

This lower-court holding serves as a reminder to businesses, particularly in regulated sectors, that the absence of a warrant does not end the inquiry as to whether the Government may access information. A search, like the search in *Naperville Smart Meter*, may nonetheless be reasonable, or another warrant exception, like exigent circumstances, might still apply.

In short, *Naperville Smart Meter* highlights the potential salience of the issues *Carpenter* explores for a variety of forms of data generation and utilization, including for infrastructure providers in particular.

* * * * *

At this point, only future court decisions will inform whether *Carpenter* is as revolutionary as some commentators have predicted or as "narrow" as the Court has suggested. Indeed, the Court's cautious approach might be seen as a recognition of the difficulty in crafting judge-made rules to govern this rapidly evolving area and, thus, as an invitation for Congress, and not the judiciary, to resolve the question of how to protect the digital tracks created by cell phone and Internet use. Congress has, in fact, played that very role in the past. The Stored Communications Act, the Foreign Intelligence Surveillance Act, and the Wiretap Act were all legislative attempts to strike an appropriate constitutional balance between privacy and security in an unsettled area of Fourth Amendment law. With this landscape in mind, and because such legislation does not appear to be imminently on the horizon, companies facing Government requests for third-party information must continue to contemplate *Carpenter* and what the decision means for their responses to those requests. inf

Endnotes

1. 138 S. Ct. 2206 (2018).
2. 18 U.S.C. § 2703(d).
3. 819 F. 3d 880 (2016).
4. *Katz v. United States*, 389 U.S. 347, 351 (1967).
5. For a similar analysis of *Carpenter*, which contributed to the factors identified in the text, see Susan Freiwald & Stephen William Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 Harv. L. Rev. 205, 219–221 (2018).
6. *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018).
7. *Id.* at 2218.
8. *Id.*
9. *Id.* at 2217 (internal quotations omitted).
10. *Id.* (internal quotations omitted).
11. *Id.* (internal quotations omitted).
12. *Id.* at 2217–18.
13. Freiwald & Smith, *supra* note 5, at 220–21.
14. 425 U.S. 435 (1976).
15. 442 U.S. 735 (1979).
16. *Carpenter*, 138 S. Ct. at 2219.
17. *Id.* at 2220 (internal quotations omitted).
18. *Id.* at 2221.
19. *Id.* at 2247 (Alito, J., dissenting).
20. *Id.* at 2221.
21. 565 U.S. 400 (2012).
22. *Carpenter*, 138 S. Ct. at 2219.
23. 134 S. Ct. 2473 (2014).
24. *Id.* at 2489.
25. *See Carpenter*, 138 S. Ct. at 2247 (Alito, J., dissenting); *see also generally* Cong. Research Serv., RL33321, Administrative Subpoenas in Criminal Investigations: A Brief Legal Analysis (2012), crsreports.congress.gov/product/pdf/RL/RL33321.
26. *Carpenter*, 138 S. Ct. at 2220.
27. *See, e.g.,* Freiwald & Smith, *supra* note 5, at 206 (noting that "*Carpenter* has been warmly welcomed as a landmark victory for privacy advocates").
28. *Katz*, 389 U.S. at 348.
29. Although the Court held in *Katz* that the content of a phone call was constitutionally protected, before *Carpenter* it had never expressly considered whether the content of emails is protected by the Fourth Amendment. The Sixth Circuit, however, had held that the Fourth Amendment does protect email content, *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), and *Carpenter* appears to endorse that position. *See Carpenter*, 138 S. Ct. at 2222 (citing *Warhsak* and strongly suggesting that the "modern-day equivalents of an individuals' own papers or effects," which would almost certainly include emails, "should receive full Fourth Amendment protection").
30. *See* David Kris, Carpenter*'s Implications for Foreign Intelligence Surveillance*, Lawfare (June 24, 2018), https://www.

lawfareblog.com/carpenters-implications-foreign-intelligence-surveillance.

31. *Carpenter*, 138 S. Ct. at 2222.

32. *Id.* at 2217 n. 3 (noting that "we need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be," since it "is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search").

33. *United States v. Blake*, No. 3:16-CR-111(JBA), 2018 WL 3974716, at *2 (D. Conn. Aug. 20, 2018) (cataloging cases relying on the "good faith" exception); *United States v. Tolbert*, No. CR-14-3761(JCH), 2018 WL 3611053, at *9 (D.N.M. July 27, 2018) (holding that *Carpenter* does not disturb traditional methods).

34. 900 F.3d 521 (7th Cir. 2018).

35. *Id.* at 527. Importantly, the Seventh Circuit noted in *Naperville Smart Meter* that there was no third-party in the traditional sense (because the citizens had turned their information directly over to the Government), but, as relevant here, it nonetheless analyzed whether *Smith* and *Miller* controlled the case.

36. *Id.* at 529.

The California Consumer Privacy Act: The First Step Towards an American GDPR?

continued from page 1

Importantly, the CCPA appears to have encouraged or accelerated the introduction of additional legislation and proposals at both the federal and state levels. Accordingly, the CCPA may prove to be the first major "canary in the coal mine" that leads to the development of a comprehensive consumer data privacy regime in the United States; the effect would be similar to the one the GDPR had on companies doing business in Europe. For this reason, and because of the expansive scope and obligations of the CCPA, it is crucial that businesses understand the law and monitor future developments in advance of the upcoming January 1, 2020, effective date.

Areas Covered by the CCPA

The CCPA broadly seeks to provide rights to California consumers with respect to their personal information, including the following:

1. the right to know what personal information a business has collected about them, where the personal information was collected from, what it is being used for, whether it is being disclosed or sold, and to whom it is being disclosed or sold;[4]
2. the right to "opt out" of allowing a business to sell their personal information to third parties (and for consumers under 16 years of age, the right not to have their personal information sold absent their, or their parent's, affirmative opt-in);[5]
3. the right to have a business delete their personal information, with some exceptions;[6] and
4. the right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act.[7]

The CCPA provides these rights to "consumers"; a consumer is defined as "a natural person who is a California resident."[8] In turn, a California "resident" includes: (1) every individual who is in California for a purpose other than one that is temporary or transitory, and (2) every individual domiciled in California who is outside the state for a temporary or transitory purpose.[9]

Consumers are granted rights with respect to their "personal information," which is broadly defined to include "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[10] The CCPA goes on to list examples of "personal information," which includes name, address, and Social Security number, but which also includes less common types of information such as "unique personal identifier, Internet Protocol address, email address, account name, [and] other similar identifiers."[11] Moreover, "personal information" even includes "inferences" that can be drawn from consumer information in order to create a consumer profile.[12] "Personal information" does not include material lawfully made available from federal, state, or local government records.[13]

The CCPA applies to for-profit businesses that collect and process the personal information of California consumers and that do business in the State of California.[14] In addition, the business must meet at least one of the following criteria for the Act to apply. The business must:

- generate annual gross revenue in excess of $25 million,
- receive or share personal information of more than 50,000 California residents annually, or
- derive at least 50 percent of its annual revenue by selling the personal information of California residents.[15]