Does it make sense that these two cases should reach different results?

37

B. DEFINING SEARCHES AND SEIZURES

1. SEARCHES

c) Searches in the Network Context

On page 431, replace Note 5 with the following new decision:

CARPENTER V. UNITED STATES

Supreme Court of the United States, 2018.
138 S.Ct. 2206.

CHIEF JUSTICE ROBERTS delivered the opinion of the Court.

This case presents the question whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements.

I

A

There are 396 million cell phone service accounts in the United States—for a Nation of 326 million people. Cell phones perform their wide and growing variety of functions by connecting to a set of radio antennas called "cell sites." Although cell sites are usually mounted on a tower, they can also be found on light posts, flagpoles, church steeples, or the sides of buildings. Cell sites typically have several directional antennas that divide the covered area into sectors.

Cell phones continuously scan their environment looking for the best signal, which generally comes from the closest cell site. Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI). The precision of this information depends on the size of the geographic area covered by the cell site. The greater the concentration of cell sites, the smaller the coverage area. As data usage from cell phones has increased, wireless carriers have installed more cell sites to handle the traffic. That has led to increasingly compact coverage areas, especially in urban areas.

Wireless carriers collect and store CSLI for their own business purposes, including finding weak spots in their network and applying "roaming" charges when another carrier routes data through their cell sites. In addition, wireless carriers often sell aggregated location records to data brokers, without individual identifying information of the sort at issue

38

here. While carriers have long retained CSLI for the start and end of incoming calls, in recent years phone companies have also collected location information from the transmission of text messages and routine data connections. Accordingly, modern cell phones generate increasingly vast amounts of increasingly precise CSLI.

B

In 2011, police officers arrested four men suspected of robbing a series of Radio Shack and (ironically enough) T-Mobile stores in Detroit. One of the men confessed that, over the previous four months, the group (along with a rotating cast of getaway drivers and lookouts) had robbed nine different stores in Michigan and Ohio. The suspect identified 15 accomplices who had participated in the heists and gave the FBI some of their cell phone numbers; the FBI then reviewed his call records to identify additional numbers that he had called around the time of the robberies.

Based on that information, the prosecutors applied for court orders under the Stored Communications Act to obtain cell phone records for petitioner Timothy Carpenter and several other suspects. That statute, as amended in 1994, permits the Government to compel the disclosure of certain telecommunications records when it "offers specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Federal Magistrate Judges issued two orders directing Carpenter's wireless carriers—MetroPCS and Sprint—to disclose cell/site sector information for Carpenter's telephone at call origination and at

call termination for incoming and outgoing calls during the four-month period when the string of robberies occurred. The first order sought 152 days of cell-site records from MetroPCS, which produced records spanning 127 days. The second order requested seven days of CSLI from Sprint, which produced two days of records covering the period when Carpenter's phone was "roaming" in northeastern Ohio. Altogether the Government obtained 12,898 location points cataloging Carpenter's movements—an average of 101 data points per day.

Carpenter was charged with six counts of robbery and an additional six counts of carrying a firearm during a federal crime of violence. At trial, seven of Carpenter's confederates pegged him as the leader of the operation. In addition, FBI agent Christopher Hess offered expert testimony about the cell-site data. Hess explained that each time a cell phone taps into the wireless network, the carrier logs a time-stamped record of the cell site and particular sector that were used. With this information, Hess produced maps that placed Carpenter's phone near four of the charged robberies. In the Government's view, the location records clinched the case: They confirmed that Carpenter was "right where the robbery was at the exact time of the robbery." App. 131 (closing argument).

39

Carpenter was convicted on all but one of the firearm counts and sentenced to more than 100 years in prison.

The Court of Appeals for the Sixth Circuit affirmed. The court held that Carpenter lacked a reasonable expectation of privacy in the location information collected by the FBI because he had shared that information with his wireless carriers. Given that cell phone users voluntarily convey cell-site data to their carriers as "a means of establishing communication," the court concluded that the resulting business records are not entitled to Fourth Amendment protection. (quoting *Smith v. Maryland,* 442 U.S. 735, 741 (1979)).

II

A

As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to "assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo v. United States,* 533 U.S. 27, 34 (2001). For that reason, we rejected in *Kyllo* a mechanical interpretation of the Fourth Amendment and held that use of a thermal imager to detect heat radiating from the side of the defendant's home was a search. Because any other conclusion would leave homeowners at the mercy of advancing technology, we determined that the Government—absent a warrant—could not capitalize on such new sense-enhancing technology to explore what was happening within the home.

Likewise in *California v. Riley,* 134 S.Ct. 2473 (2014), the Court recognized the immense storage capacity of modern cell phones in holding that police officers must generally obtain a warrant before searching the contents of a phone. We explained that while the general rule allowing warrantless searches incident to arrest strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to the vast store of sensitive information on a cell phone.

B

The case before us involves the Government's acquisition of wireless carrier cell-site records revealing the location of Carpenter's cell phone whenever it made or received calls. This sort of digital data—personal location information maintained by a third party—does not fit neatly under existing precedents. Instead, requests for cell-site records lie at the intersection of two lines of cases, both of which inform our understanding of the privacy interests at stake.

The first set of cases addresses a person's expectation of privacy in his physical location and movements. In *United States v. Knotts,* 460 U.S. 276 (1983), we considered the Government's use of a "beeper" to aid in tracking a vehicle through traffic. Police officers in that case planted a beeper in a

40

container of chloroform before it was purchased by one of Knotts's co-conspirators. The officers (with intermittent aerial assistance) then followed the automobile carrying the container from Minneapolis to Knotts's cabin in Wisconsin, relying on the beeper's signal to help keep the vehicle in view. The Court concluded that the augmented visual surveillance did not constitute a search because a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. Since the movements of the vehicle and its final destination had been voluntarily conveyed to anyone who wanted to look, Knotts could not assert a privacy interest in the information obtained.

This Court in *Knotts,* however, was careful to distinguish between the rudimentary tracking facilitated by the beeper

and more sweeping modes of surveillance. The Court emphasized the limited use which the government made of the signals from this particular beeper during a discrete automotive journey. Significantly, the Court reserved the question whether different constitutional principles may be applicable if twenty-four hour surveillance of any citizen of this country were possible.

Three decades later, the Court considered more sophisticated surveillance of the sort envisioned in *Knotts* and found that different principles did indeed apply. In *United States v. Jones,* 565 U.S. 400 (2012), FBI agents installed a GPS tracking device on Jones's vehicle and remotely monitored the vehicle's movements for 28 days. The Court decided the case based on the Government's physical trespass of the vehicle. At the same time, five Justices agreed that related privacy concerns would be raised by, for example, surreptitiously activating a stolen vehicle detection system in Jones's car to track Jones himself, or conducting GPS tracking of his cell phone. *Id.,* at 426, 428 (Alito, J., concurring in judgment); *id.,* at 415 (Sotomayor, J., concurring). Since GPS monitoring of a vehicle tracks every movement a person makes in that vehicle, the concurring Justices concluded that longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy—regardless whether those movements were disclosed to the public at large. *Id.,* at 430, (opinion of Alito, J.); *id.,* at 415 (opinion of Sotomayor, J.).

In a second set of decisions, the Court has drawn a line between what a person keeps to himself and what he shares with others. We have previously held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties. *Smith v. Maryland,* 442 U.S. 735, 743–744 (1979). That remains true even if the information is revealed on the assumption that it will be used only for a limited purpose. *United States v. Miller,* 425 U.S. 435, 443 (1976). As a result, the Government is typically free to obtain such information from the recipient without triggering Fourth Amendment protections.

41

This third-party doctrine largely traces its roots to *Miller*. While investigating Miller for tax evasion, the Government subpoenaed his banks, seeking several months of canceled checks, deposit slips, and monthly statements. The Court rejected a Fourth Amendment challenge to the records collection. For one, Miller could assert neither ownership nor possession of the documents; they were business records of the banks. For another, the nature of those records confirmed Miller's limited expectation of privacy, because the checks were not confidential communications but negotiable instruments to be used in commercial transactions, and the bank statements contained information exposed to bank employees in the ordinary course of business. The Court thus concluded that Miller had taken the risk, in revealing his affairs to another, that the information would be conveyed by that person to the Government.

Three years later, *Smith* applied the same principles in the context of information conveyed to a telephone company. The Court ruled that the Government's use of a pen register—a device that recorded the outgoing phone numbers dialed on a landline telephone—was not a search. Noting the pen register's limited capabilities, the Court doubted that people in general entertain any actual expectation of privacy in the numbers they dial. Telephone subscribers know, after all, that the numbers are used by the telephone company for a variety of legitimate business purposes, including routing calls. And at any rate, the Court explained, such an expectation is not one that society is prepared to recognize as reasonable. When Smith placed a call, he voluntarily conveyed the dialed numbers to the phone company by exposing that information to its equipment in the ordinary course of business. Once again, we held that the defendant assumed the risk that the company's records would be divulged to police.

III

The question we confront today is how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals. Such tracking partakes of many of the qualities of the GPS monitoring we considered in *Jones*. Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled.

At the same time, the fact that the individual continuously reveals his location to his wireless carrier implicates the third-party principle of *Smith* and *Miller*. But while the third-party doctrine applies to telephone numbers and bank records, it is not clear whether its logic extends to the qualitatively different category of cell-site records. After all, when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements.

42

We decline to extend *Smith* and *Miller* to cover these novel circumstances. Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection. Whether the Government employs its own surveillance technology as in *Jones* or leverages the

technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. The location information obtained from Carpenter's wireless carriers was the product of a search.[3]

A

A person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, what one seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected. A majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements. *Jones*, 565 U.S., at 430 (Alito, J., concurring in judgment); *id.*, at 415 (Sotomayor, J., concurring). Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so for any extended period of time was difficult and costly and therefore rarely undertaken. For that reason, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.

Allowing government access to cell-site records contravenes that expectation. Although such records are generated for commercial purposes, that distinction does not negate Carpenter's anticipation of privacy in his physical location. Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data 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. These location records hold for many Americans the privacies of life. And like GPS monitoring, cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense.

In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones*.

43

Unlike the bugged container in *Knotts* or the car in *Jones*, a cell phone—almost a feature of human anatomy—tracks nearly exactly the movements of its owner. While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales. Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user.

Moreover, the retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers, which currently maintain records for up to five years. Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone. Unlike with the GPS device in *Jones*, police need not even know in advance whether they want to follow a particular individual, or when.

Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may—in the Government's view—call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance.

The Government and Justice Kennedy contend [in dissent] that the collection of CSLI should be permitted because the data is less precise than GPS information. Not to worry, they maintain, because the location records did not on their own suffice to place Carpenter at the crime scene; they placed him within a wedge-shaped sector ranging from one-eighth to four square miles. . . . [But] the rule the Court adopts must take account of more sophisticated systems that are already in use or in development. While the records in this case reflect the state of technology at the start of the decade, the accuracy of CSLI is rapidly approaching GPS-level precision. As the number of cell sites has proliferated, the geographic area covered by each cell sector has shrunk, particularly in urban areas. In addition, with new technology measuring the time and angle of signals hitting their towers, wireless carriers already have the capability to pinpoint a phone's location within 50 meters. Brief for Electronic Frontier Foundation et al. as *Amici Curiae* 12 (describing triangulation methods that estimate a device's location inside a given cell sector).

44

Accordingly, when the Government accessed CSLI from the wireless carriers, it invaded Carpenter's reasonable

expectation of privacy in the whole of his physical movements.

B

The Government's primary contention to the contrary is that the third-party doctrine governs this case. In its view, cell-site records are fair game because they are "business records" created and maintained by the wireless carriers. The Government (along with Justice Kennedy) recognizes that this case features new technology, but asserts that the legal question nonetheless turns on a garden-variety request for information from a third-party witness.

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. Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible. 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. The Government thus is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information.

The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another. But the fact of diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely. *Smith* and *Miller,* after all, did not rely solely on the act of sharing. Instead, they considered the nature of the particular documents sought to determine whether there is a legitimate 'expectation of privacy' concerning their contents. *Smith* pointed out the limited capabilities of a pen register; as explained in *Riley,* telephone call logs reveal little in the way of identifying information. *Miller* likewise noted that checks were not confidential communications but negotiable instruments to be used in commercial transactions. In mechanically applying the third-party doctrine to this case, the Government fails to appreciate that there are no comparable limitations on the revealing nature of CSLI.

The Court has in fact already shown special solicitude for location information in the third-party context. In *Knotts,* the Court relied on *Smith* to hold that an individual has no reasonable expectation of privacy in public movements that he "voluntarily conveyed to anyone who wanted to look. But when confronted with more pervasive tracking, five Justices [in *Jones*] agreed that longer term GPS monitoring of even a vehicle traveling on

45

public streets constitutes a search. [T]his case is not about "using a phone" or a person's movement at a particular time. It is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years. Such a chronicle implicates privacy concerns far beyond those considered in *Smith* and *Miller*.

Neither does the second rationale underlying the third-party doctrine—voluntary exposure—hold up when it comes to CSLI. Cell phone location information is not truly "shared" as one normally understands the term. In the first place, 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. Second, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily assume the risk of turning over a comprehensive dossier of his physical movements.

We therefore decline to extend *Smith* and *Miller* to the collection of CSLI. Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection. The Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment.

* * *

Our decision today is a 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.

As Justice Brandeis explained in his famous dissent, the Court is obligated—as "subtler and more far-reaching means of invading privacy have become available to the Government"—to ensure that the "progress of science" does not erode Fourth Amendment protections. *Olmstead v. United States,* 277 U.S. 438, 473–474 (1928). Here the progress of science has afforded law enforcement a powerful new tool to carry out its important responsibilities. At the same time, this tool risks

Government

46

encroachment of the sort the Framers, after consulting the lessons of history, drafted the Fourth Amendment to prevent.

We decline to grant the state unrestricted access to a wireless carrier's database of physical location information. In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection. The Government's acquisition of the cell-site records here was a search under that Amendment.

JUSTICE KENNEDY, with whom JUSTICE THOMAS and JUSTICE ALITO join, dissenting.

This case involves new technology, but the Court's stark departure from relevant Fourth Amendment precedents and principles is, in my submission, unnecessary and incorrect, requiring this respectful dissent.

The new rule the Court seems to formulate puts needed, reasonable, accepted, lawful, and congressionally authorized criminal investigations at serious risk in serious cases, often when law enforcement seeks to prevent the threat of violent crimes. And it places undue restrictions on the lawful and necessary enforcement powers exercised not only by the Federal Government, but also by law enforcement in every State and locality throughout the Nation. Adherence to this Court's longstanding precedents and analytic framework would have been the proper and prudent way to resolve this case.

The Court has twice held that individuals have no Fourth Amendment interests in business records which are possessed, owned, and controlled by a third party. *United States v. Miller,* 425 U.S. 435 (1976); *Smith v. Maryland,* 442 U.S. 735 (1979). This is true even when the records contain personal and sensitive information. So when the Government uses a subpoena to obtain, for example, bank records, telephone records, and credit card statements from the businesses that create and keep these records, the Government does not engage in a search of the business's customers within the meaning of the Fourth Amendment.

Petitioner acknowledges that the Government may obtain a wide variety of business records using compulsory process, and he does not ask the Court to revisit its precedents. Yet he argues that, under those same precedents, the Government searched his records when it used court-approved compulsory process to obtain the cell-site information at issue here. Cell-site records, however, are no different from the many other kinds of business records the Government has a lawful right to obtain by compulsory process. Customers like petitioner do not own, possess, control, or use the records, and for that reason have no reasonable expectation that they cannot be disclosed pursuant to lawful compulsory process.

47

The Court today disagrees. It holds for the first time that by using compulsory process to obtain records of a business entity, the Government has not just engaged in an impermissible action, but has conducted a search of the business's customer. The Court further concludes that the search in this case was unreasonable and the Government needed to get a warrant to obtain more than six days of cell-site records.

In concluding that the Government engaged in a search, the Court unhinges Fourth Amendment doctrine from the property-based concepts that have long grounded the analytic framework that pertains in these cases. In doing so it draws an unprincipled and unworkable line between cell-site records on the one hand and financial and telephonic records on the other. According to today's majority opinion, the Government can acquire a record of every credit card purchase and phone call a person makes over months or years without upsetting a legitimate expectation of privacy. But, in the Court's view, the Government crosses a constitutional line when it obtains a court's approval to issue a subpoena for more than six days of cell-site records in order to determine whether a person was within several hundred city blocks of a crime scene. That distinction is illogical and will frustrate principled application of the Fourth Amendment in many routine yet vital law enforcement operations.

It is true that the Cyber Age has vast potential both to expand and restrict individual freedoms in dimensions not contemplated in earlier times. However, there is simply no basis here for concluding that the Government interfered with information that the cell phone customer, either from a legal or commonsense standpoint, should have thought the law would deem owned or controlled by him.

JUSTICE GORSUCH, dissenting.

Today the Court suggests that *Smith* and *Miller* distinguish between *kinds* of information disclosed to third parties and require courts to decide whether to "extend" those decisions to particular classes of information, depending on their

sensitivity. But as the Sixth Circuit recognized and Justice Kennedy explains, no balancing test of this kind can be found in *Smith* and *Miller*. Those cases announced a categorical rule: Once you disclose information to third parties, you forfeit any reasonable expectation of privacy you might have had in it. And even if *Smith* and *Miller* did permit courts to conduct a balancing contest of the kind the Court now suggests, it's still hard to see how that would help the petitioner in this case. Why is someone's location when using a phone so much more sensitive than who he was talking to (*Smith*) or what financial transactions he engaged in (*Miller*)? I do not know and the Court does not say.

I cannot fault the Sixth Circuit for holding that *Smith* and *Miller* extinguish any *Katz*-based Fourth Amendment interest in third party cell-site data. That is the plain effect of their categorical holdings. Nor can I

48

fault the Court today for its implicit but unmistakable conclusion that the rationale of *Smith* and *Miller* is wrong; indeed, I agree with that. The Sixth Circuit was powerless to say so, but this Court can and should. At the same time, I do not agree with the Court's decision today to keep *Smith* and *Miller* on life support and supplement them with a new and multilayered inquiry that seems to be only *Katz*-squared. Returning there, I worry, promises more trouble than help. Instead, I would look to a more traditional Fourth Amendment approach. Even if *Katz* may still supply one way to prove a Fourth Amendment interest, it has never been the only way. Neglecting more traditional approaches may mean failing to vindicate the full protections of the Fourth Amendment.

Notes and Questions

1. *New versus traditional surveillance techniques*. The Supreme Court's *Carpenter* decision draws a distinction between new technologies that cause "seismic shifts" in the government's power and "traditional surveillance techniques" that are not called into question by the Court's reasoning. On one hand, *Carpenter* directs that use of "seismic shift" technologies can be a search to prevent the government from having too much surveillance power as a result of technological change. On the other hand, *Carpenter* suggests that traditional surveillance techniques that were not a search under traditional Fourth Amendment principles remain a non-search. How should courts apply this distinction to Internet surveillance?

2. *Translating Carpenter's physical expectations to the Internet*. *Carpenter* is based on an understanding of traditional expectations in the physical world. In the past, the Court reasons, you wouldn't expect others to monitor your every single movement in physical space for a long period of time because it would be technologically impossible. New technology has changed that expectation, *Carpenter* explains. Technology has enabled perfect location surveillance that previously didn't exist. The law must declare that monitoring a search, the Court reasons, to restore the earlier balance of government power.

But how does that apply to Internet surveillance? There is likely no established past set of societal expectations about how much Internet surveillance power the government has. Given that, how can you tell if technological changes in Internet surveillance power have changed a previous expectation? Or is the idea that the entire Internet, viewed as a whole, works a "seismic shift" in the amount of surveillance power the government has relative to the pre-Internet age? If so, what were the old expectations about government power, and what is the new reality? And what legal rules are needed to restore the old reality of government power by changing Fourth Amendment doctrine?

3. *Carpenter and collecting IP addresses*. The post-*Carpenter* cases on surveillance of IP addresses have so far concluded that collecting the IP address that an account is using to connect to the Internet is not a search. Consider the First Circuit's reasoning in United States v. Hood, 920 F.3d 87

49

(1st Cir. 2019). In *Hood*, the government had reason to believe that someone using a particular Kik account with the associated name "Rusty Hood" had recently used the account to commit a crime. In an effort to identify the suspect, investigators asked Kik to disclose the IP addresses used to log in to the account recently. Kik disclosed the IP addresses used over a four-day period, and that led to the identification and prosecution of the user, Mr. Rusty Hood. Hood argued that obtaining his IP addresses was a Fourth Amendment search under *Carpenter*. The First Circuit disagreed:

> An internet user generates the IP address data that the government acquired from Kik in this case only by making the affirmative decision to access a website or application. By contrast, as the Supreme Court noted in *Carpenter*, every time a cell phone receives a call, text message, or email, the cell phone pings CSLI to the nearest cell site tower without the cell phone user lifting a finger. In fact, those pings are recorded every time a cell phone application updates of its own accord, possibly to refresh a news feed or generate new weather data, such that even a cell phone sitting untouched in a suspect's pocket is continually chronicling that user's movements throughout the day.
>
> Moreover, the IP address data that the government acquired from Kik does not itself convey any location information. The IP address data is merely a string of numbers associated with a device that had, at one time, accessed a wireless network.

> By contrast, CSLI itself reveals—without any independent investigation—the (at least approximate) location of the cell phone user who generates that data simply by possessing the phone.
>
> Thus, the government's warrantless acquisition from Kik of the IP address data at issue here in no way gives rise to the unusual concern that the Supreme Court identified in *Carpenter* that, if the third-party doctrine were applied to the acquisition of months of Carpenter's CSLI, only the few without cell phones could escape tireless and absolute surveillance. Accordingly, we conclude that Hood did not have a reasonable expectation of privacy in the information that the government acquired from Kik without a warrant.

Id. at 91–92. *See also* United States v. Morel, 922 F.3d 1 (1st Cir. 2019); United States v. Wellbeloved-Stone, 777 Fed.Appx. 605 (4th Cir. 2019). Do you agree?

Also consider how *Carpenter* might apply to the facts of *United States v. Forrester* on pages 425–28 of your casebook. In *Forrester*, the government monitored a home Internet connection and obtained the IP addresses of the websites visited from the account. Note the key difference between the facts of *Forrester* and the facts of *Hood*. In *Hood*, the IP addresses collected were Hood's assigned IP addresses. In *Forrester*, the IP addresses collected were those visited from the home's account. Should that make a difference? Is the government's power to observe the address of every website a person visits over

50

time a new power that has caused a "seismic shift" in government power? Or is IP address monitoring merely a "traditional" surveillance technique because IP addresses are just the Internet version of telephone numbers dialed?

4. *Short-term vs. long-term surveillance*. Footnote 3 of *Carpenter* states that the Court "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." The distinction between long-term and short-term surveillance was the basis of Justice Alito's concurring opinion in *Jones,* on which the reasoning of *Carpenter* is based. In *Jones*, the government installed a physical GPS device on a car the suspect was driving and tracked the car's location for 28 days. Justice Alito reasoned that using the GPS device only briefly was not a search because that was the kind of government surveillance people have traditionally expected. Longer term surveillance became a search, Justice Alito reasoned, because it was the kind of surveillance that people wouldn't expect the government to be able to conduct. Here's the key language from Justice Alito's *Jones* concurrence:

> Relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving.
>
> We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark. Other cases may present more difficult questions. But where uncertainty exists with respect to whether a certain period of GPS surveillance is long enough to constitute a Fourth Amendment search, the police may always seek a warrant. We also need not consider whether prolonged GPS monitoring in the context of investigations involving extraordinary offenses would similarly intrude on a constitutionally protected sphere of privacy. In such cases, long-term tracking might have been mounted using previously available techniques.
>
> For these reasons, I conclude that the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment.

United States v. Jones, 565 U.S. 400, 430–31 (Alito, J., concurring in the judgment).

If *Carpenter* is based on the reasoning of Justice Alito's *Jones* concurrence, does that mean that some kind of short-term collection of CSLI is not a search?

51

If so, how short is short enough not to be a search? In Kinslow v. State, 2019 WL 2440229 (Ind. Ct. App. 2019), investigators placed a GPS device inside a package that Kinslow later picked up and placed in his car. The police tracked the location of Kinslow's car as it drove around for about six hours. The Indiana Court of Appeals held that no search occurred under *Carpenter*:

> While the United States Supreme Court found that tracking such information violated Carpenter's expectation of privacy, we read the Court's holding to apply to records, such as cellphone tracking data, that hold for many Americans the 'privacies of life.' Cell phone location data provides an intimate window into a person's life, revealing not only his particular movements, but through them his professional, political, religious, and sexual associations. Because the tracking

> of Kinslow lasted only approximately six hours and because the electronic devices used here do not provide an intimate window into a person's life, we find that *Carpenter* has no bearing on this case.

Id. at *3 n.6. *See also* Sims v. State, 569 S.W.3d 634 (Tex. Ct. Crim. App. 2019) (holding that *Carpenter* applies to real-time cell-site pinging, but that obtaining real-time location with five pings over less than three hours was insufficient to trigger a *Carpenter* search).

C. EXCEPTIONS TO THE WARRANT REQUIREMENT

2. EXIGENT CIRCUMSTANCES

At the top of page 477, before the beginning of Section 3, add the following new Notes 5 and 6:

5. *When does seizing a computer for too long without a warrant justify suppression of the evidence found inside it?* In United States v. Jobe, 933 F.3d 1074 (9th Cir. 2019), the Ninth Circuit added a wrinkle to the question of how long an officer can seize a computer before obtaining a warrant to search it. Even if a computer was seized and held for an overly long period, the court reasoned, the good-faith exception to the exclusionary rule may apply if the extended period of the warrantless seizure was not particularly culpable and the officer reasonably believed the seizure was reasonable. In that setting, there may be no suppression remedy for the failure to obtain a warrant promptly. *Id*. at 1079–80.

If *Jobe* is correct that the good-faith exception can apply in these circumstances, how much more time should the good-faith exception add to the period over which a warrantless seizure of a computer is effectively allowed?

6. *Exigent circumstances requires reason to believe digital evidence will be destroyed or concealed*. In Hupp v. Cook, 931 F.3d 307 (4th Cir. 2019), Trooper Cook testified that he had a regular practice of seizing any computer or cell phone that he believed might contain video of a crime he was

investigating. He did this, he claimed, because digital evidence can be easily deleted or destroyed. The Fourth Circuit concluded that Trooper Cook's regular practice was not permitted by the exigent circumstances exception:

> In an era in which cell phones are increasingly used to capture much of what happens in daily life, it is important to emphasize the limitations that the Fourth Amendment continues to place on a state's seizure of video evidence.
>
> The exigent circumstances exception does not permit police officers to do what Trooper Cook routinely does: seize video evidence without a warrant even when there is no reason to believe that the evidence will likely be destroyed or concealed. Such a rule would allow officers to seize as a matter of course video-recording devices from not just those involved in an incident, but also from neighbors and other curious bystanders who happen to record the events as they transpire. Under this view, police officers would lawfully be permitted to enter the home of every person living nearby who stands in her doorway or window recording an arrest, to seize her recording device, and to do so without a warrant or her consent—simply because video evidence, by its nature, can be easily deleted.
>
> Such a view finds no support in our Fourth Amendment jurisprudence. While video evidence contained in a cell phone can be easily deleted or concealed, it is not merely the ease with which evidence may be destroyed or concealed that dictates exigency. An officer must also have reason to believe that the evidence will be destroyed or concealed. In short, adopting the broad definition of exigency urged by Trooper Cook would remove the exigent circumstances exception to the warrant requirement from the class of narrow and well-delineated exceptions permissible under the Fourth Amendment. It would convert exigency from an exception to the rule.

Id. at 329–30.

4. BORDER SEARCHES

At the bottom of page 517, add the following new Notes 8, 9, and 10:

8. *Federal circuits divide on applying the border search exception to computers*. Recent decisions from the Fourth Circuit and Eleventh Circuit have reached different conclusions on how to apply the border exception to computers. The new decisions create a clear disagreement among lower courts that may prompt review from the United States Supreme Court.

First, in United States v. Kolsuz, 890 F.3d 133 (4th Cir. 2018), the Fourth Circuit held that forensic searches of computers at the border require some kind of suspicion. The Fourth Circuit's decision, authored by Judge Pamela