Syllabus

NOTE: Where it is feasible, a syllabus (headnote) will be released, as is being done in connection with this case, at the time the opinion is issued. The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States* v. *Detroit Timber & Lumber Co.,* 200 U. S. 321, 337.

SUPREME COURT OF THE UNITED STATES

Syllabus

CARPENTER *v.* UNITED STATES

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

No. 16–402. Argued November 29, 2017—Decided June 22, 2018

Cell phones perform their wide and growing variety of functions by continuously connecting to a set of radio antennas called "cell sites." Each time a phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI). Wireless carriers collect and store this information for their own business purposes. Here, after the FBI identified the cell phone numbers of several robbery suspects, prosecutors were granted court orders to obtain the suspects' cell phone records under the Stored Communications Act. Wireless carriers produced CSLI for petitioner Timothy Carpenter's phone, and the Government was able to obtain 12,898 location points cataloging Carpenter's movements over 127 days—an average of 101 data points per day. Carpenter moved to suppress the data, arguing that the Government's seizure of the records without obtaining a warrant supported by probable cause violated the Fourth Amendment. The District Court denied the motion, and prosecutors used the records at trial to show that Carpenter's phone was near four of the robbery locations at the time those robberies occurred. Carpenter was convicted. The Sixth Circuit affirmed, holding 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.

Held:

1. The Government's acquisition of Carpenter's cell-site records was a Fourth Amendment search. Pp. 4–18.

(a) The Fourth Amendment protects not only property interests but certain expectations of privacy as well. *Katz* v. *United States,* 389 U. S. 347, 351. Thus, when an individual "seeks to preserve something as private," and his expectation of privacy is "one that society is

prepared to recognize as reasonable," official intrusion into that sphere generally qualifies as a search and requires a warrant supported by probable cause. *Smith* v. *Maryland*, 442 U. S. 735, 740 (internal quotation marks and alterations omitted). The analysis regarding which expectations of privacy are entitled to protection is informed by historical understandings "of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted." *Carroll* v. *United States,* 267 U. S. 132, 149. These Founding-era understandings continue to inform this Court when applying the Fourth Amendment to innovations in surveillance tools. See, *e.g., Kyllo* v. *United States,* 533 U. S. 27. Pp. 4–7.

(b) The digital data at issue—personal location information maintained by a third party—does not fit neatly under existing precedents but lies at the intersection of two lines of cases. One set addresses a person's expectation of privacy in his physical location and movements. See, *e.g., United States* v. *Jones,* 565 U. S. 400 (five Justices concluding that privacy concerns would be raised by GPS tracking). The other addresses a person's expectation of privacy in information voluntarily turned over to third parties. See *United States* v. *Miller,* 425 U. S. 435 (no expectation of privacy in financial records held by a bank), and *Smith,* 442 U. S. 735 (no expectation of privacy in records of dialed telephone numbers conveyed to telephone company). Pp. 7–10.

(c) Tracking a person's past movements through CSLI partakes of many of the qualities of GPS monitoring considered in *Jones*—it is detailed, encyclopedic, and effortlessly compiled. At the same time, however, the fact that the individual continuously reveals his location to his wireless carrier implicates the third-party principle of *Smith* and *Miller*. Given the unique nature of cell-site records, this Court declines to extend *Smith* and *Miller* to cover them. Pp. 10–18.

(1) A majority of the Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements. Allowing government access to cell-site records—which "hold for many Americans the 'privacies of life,'" *Riley* v. *California*, 573 U. S. ___, ___—contravenes that expectation. In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring considered in *Jones*: They give the Government near perfect surveillance and allow it to travel back in time to retrace a person's whereabouts, subject only to the five-year retention policies of most wireless carriers. The Government contends that CSLI data is less precise than GPS information, but it thought the data accurate enough here to highlight it during closing argument in Carpenter's trial. At any rate, the rule the Court adopts "must take account of more sophisticated systems that are already in use or in

development," *Kyllo*, 533 U. S., at 36, and the accuracy of CSLI is rapidly approaching GPS-level precision. Pp. 12–15.

(2) The Government contends that the third-party doctrine governs this case, because cell-site records, like the records in *Smith* and *Miller*, are "business records," created and maintained by wireless carriers. But 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.

The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another. *Smith* and *Miller*, however, did not rely solely on the act of sharing. They also considered "the nature of the particular documents sought" and limitations on any "legitimate 'expectation of privacy' concerning their contents." *Miller*, 425 U. S., at 442. In mechanically applying the third-party doctrine to this case the Government fails to appreciate the lack of comparable limitations on the revealing nature of CSLI.

Nor does the second rationale for the third-party doctrine—voluntary exposure—hold up when it comes to CSLI. Cell phone location information is not truly "shared" as the term is normally understood. First, 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. *Riley*, 573 U. S., at ___. Second, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the user's part beyond powering up. Pp. 15–17.

(d) This decision is narrow. It does not express a view on matters not before the Court; does not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras; does not address other business records that might incidentally reveal location information; and does not consider other collection techniques involving foreign affairs or national security. Pp. 17–18.

2. The Government did not obtain a warrant supported by probable cause before acquiring Carpenter's cell-site records. It acquired those records pursuant to a court order under the Stored Communications Act, which required the Government to show "reasonable grounds" for believing that the records were "relevant and material to an ongoing investigation." 18 U. S. C. §2703(d). That showing falls well short of the probable cause required for a warrant. Consequently, an order issued under §2703(d) is not a permissible mechanism for accessing historical cell-site records. Not all orders compelling the production of documents will require a showing of probable cause. A

Syllabus

warrant is required only in the rare case where the suspect has a legitimate privacy interest in records held by a third party. And even though the Government will generally need a warrant to access CSLI, case-specific exceptions—*e.g.*, exigent circumstances—may support a warrantless search. Pp. 18–22.

819 F. 3d 880, reversed and remanded.

ROBERTS, C. J., delivered the opinion of the Court, in which GINSBURG, BREYER, SOTOMAYOR, and KAGAN, JJ., joined. KENNEDY, J., filed a dissenting opinion, in which THOMAS and ALITO, JJ., joined. THOMAS, J., filed a dissenting opinion. ALITO, J., filed a dissenting opinion, in which THOMAS, J., joined. GORSUCH, J., filed a dissenting opinion.

SUPREME COURT OF THE UNITED STATES

No. 16–402

TIMOTHY IVORY CARPENTER, PETITIONER *v.* UNITED STATES

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

[June 22, 2018]

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 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. App. to Pet. for Cert. 60a, 72a. 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. See 18 U. S. C. §§924(c), 1951(a). Prior to trial, Carpenter moved to suppress the cell-site data provided by the wireless carriers. He argued that the Government's seizure of the records violated the Fourth Amendment because they had been obtained without a warrant supported by probable cause. The District Court denied the motion. App. to Pet. for Cert. 38a–39a.

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). 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. 819 F. 3d 880 (2016). 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. *Id.,* at 888 (quoting *Smith* v. *Maryland*, 442 U. S. 735, 741 (1979)).

We granted certiorari. 582 U. S. ___ (2017).

II

A

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The "basic purpose of this Amendment," our cases have recognized, "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Camara* v. *Municipal Court of City and County of San Francisco*, 387 U. S. 523, 528 (1967). The Founding generation crafted the Fourth Amendment as a "response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rum-

mage through homes in an unrestrained search for evidence of criminal activity." *Riley* v. *California*, 573 U. S. ___, ___ (2014) (slip op., at 27). In fact, as John Adams recalled, the patriot James Otis's 1761 speech condemning writs of assistance was "the first act of opposition to the arbitrary claims of Great Britain" and helped spark the Revolution itself. *Id.,* at ___–___ (slip op., at 27–28) (quoting 10 Works of John Adams 248 (C. Adams ed. 1856)).

For much of our history, Fourth Amendment search doctrine was "tied to common-law trespass" and focused on whether the Government "obtains information by physically intruding on a constitutionally protected area." *United States* v. *Jones*, 565 U. S. 400, 405, 406, n. 3 (2012). More recently, the Court has recognized that "property rights are not the sole measure of Fourth Amendment violations." *Soldal* v. *Cook County*, 506 U. S. 56, 64 (1992). In *Katz* v. *United States*, 389 U. S. 347, 351 (1967), we established that "the Fourth Amendment protects people, not places," and expanded our conception of the Amendment to protect certain expectations of privacy as well. When an individual "seeks to preserve something as private," and his expectation of privacy is "one that society is prepared to recognize as reasonable," we have held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause. *Smith*, 442 U. S., at 740 (internal quotation marks and alterations omitted).

Although no single rubric definitively resolves which expectations of privacy are entitled to protection,[1] the

---

[1] JUSTICE KENNEDY believes that there is such a rubric—the "property-based concepts" that *Katz* purported to move beyond. *Post,* at 3 (dissenting opinion). But while property rights are often informative, our cases by no means suggest that such an interest is "fundamental" or "dispositive" in determining which expectations of privacy are legitimate. *Post,* at 8–9. JUSTICE THOMAS (and to a large extent JUSTICE GORSUCH) would have us abandon *Katz* and return to an

analysis is informed by historical understandings "of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted." *Carroll* v. *United States*, 267 U. S. 132, 149 (1925). On this score, our cases have recognized some basic guideposts. First, that the Amendment seeks to secure "the privacies of life" against "arbitrary power." *Boyd* v. *United States*, 116 U. S. 616, 630 (1886). Second, and relatedly, that a central aim of the Framers was "to place obstacles in the way of a too permeating police surveillance." *United States* v. *Di Re*, 332 U. S. 581, 595 (1948).

We have kept this attention to Founding-era understandings in mind when applying the Fourth Amendment to innovations in surveillance tools. 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. *Id.,* at 35. 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

---

exclusively property-based approach. *Post,* at 1–2, 17–21 (THOMAS J., dissenting); *post,* at 6–9 (GORSUCH, J., dissenting). *Katz* of course "discredited" the "premise that property interests control," 389 U. S., at 353, and we have repeatedly emphasized that privacy interests do not rise or fall with property rights, see, *e.g., United States* v. *Jones*, 565 U. S. 400, 411 (2012) (refusing to "make trespass the exclusive test"); *Kyllo* v. *United States*, 533 U. S. 27, 32 (2001) ("We have since decoupled violation of a person's Fourth Amendment rights from trespassory violation of his property."). Neither party has asked the Court to reconsider *Katz* in this case.

what was happening within the home. *Ibid.*

Likewise in *Riley*, 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. 573 U. S., at ___ (slip op., at 17). 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. *Id.*, at ___ (slip op., at 9).

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 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 "augment[ed]" 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." *Id.,* at 281, 282. 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. *Id.,* at 281.

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." *Id.,* at 284, 285. 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." *Id.,* at 283–284.

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*, 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. 565 U. S., at 404–405. 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.).[2]

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,* 442 U. S., at 743–744. 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.

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." *Id.,* at 440. 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

---

[2]JUSTICE KENNEDY argues that this case is in a different category from *Jones* and the dragnet-type practices posited in *Knotts* because the disclosure of the cell-site records was subject to "judicial authorization." *Post*, at 14–16. That line of argument conflates the threshold question whether a "search" has occurred with the separate matter of whether the search was reasonable. The subpoena process set forth in the Stored Communications Act does not determine a target's expectation of privacy. And in any event, neither *Jones* nor *Knotts* purported to resolve the question of what authorization may be required to conduct such electronic surveillance techniques. But see *Jones*, 565 U. S., at 430 (ALITO, J., concurring in judgment) (indicating that longer term GPS tracking may require a warrant).

[bank] employees in the ordinary course of business." *Id.,* at 442. The Court thus concluded that Miller had "take[n] the risk, in revealing his affairs to another, that the information [would] be conveyed by that person to the Government." *Id.,* at 443.

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 "doubt[ed] that people in general entertain any actual expectation of privacy in the numbers they dial." 442 U. S., at 742. Telephone subscribers know, after all, that the numbers are used by the telephone company "for a variety of legitimate business purposes," including routing calls. *Id.,* at 743. And at any rate, the Court explained, such an expectation "is not one that society is prepared to recognize as reasonable." *Ibid.* (internal quotation marks omitted). When Smith placed a call, he "voluntarily conveyed" the dialed numbers to the phone company by "expos[ing] that information to its equipment in the ordinary course of business." *Id.,* at 744 (internal quotation marks omitted). Once again, we held that the defendant "assumed the risk" that the company's records "would be divulged to police." *Id.,* at 745.

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.

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]

---

[3]The parties suggest as an alternative to their primary submissions that the acquisition of CSLI becomes a search only if it extends beyond a limited period. See Reply Brief 12 (proposing a 24-hour cutoff); Brief for United States 55–56 (suggesting a seven-day cutoff). As part of its argument, the Government treats the seven days of CSLI requested from Sprint as the pertinent period, even though Sprint produced only two days of records. Brief for United States 56. Contrary to JUSTICE KENNEDY's assertion, *post,* at 19, 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. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.

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." *Katz*, 389 U. S., at 351–352. 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." *Id.,* at 429 (opinion of ALITO, J.). 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." *Id.*, at 430.

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." *Id.,* at 415 (opinion of SOTOMAYOR, J.). These location records "hold for many Americans the 'privacies of life.'" *Riley*, 573 U. S., at ___ (slip op., at 28) (quoting *Boyd*, 116 U. S., at 630). 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*. Unlike the bugged container in *Knotts* or the car in *Jones*, a cell phone—almost a "feature of human anatomy," *Riley*, 573 U. S., at ___ (slip op., at 9)—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. See *id.*, at ___ (slip op., at 19) (noting that "nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower"); contrast *Cardwell* v. *Lewis*, 417 U. S. 583, 590 (1974) (plurality opinion) ("A car has little capacity for escaping public scrutiny."). 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, however, 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. Brief for United States 24; see *post,* at 18–19. Yet the Court has already rejected the proposition that "inference insulates a search." *Kyllo*, 533 U. S., at 36. From the 127 days of location data it received, the Government could, in combination with other information, deduce a detailed log of Carpenter's movements, including when he was at the site of the robberies. And the Government thought the CSLI accurate enough to highlight it during the closing argument of his trial. App. 131.

At any rate, the rule the Court adopts "must take account of more sophisticated systems that are already in use or in development." *Kyllo*, 533 U. S., at 36. 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).

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. Brief for United States 32–34; *post,* at 12–14.

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." *Riley*, 573 U. S., at ___ (slip op., at 16). *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." *Miller*, 425 U. S., at 442. *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." *Smith*, 442 U. S., at 742; *Riley*, 573 U. S., at ___ (slip op., at 24). *Miller* likewise noted that checks were "not confidential communications but negotiable instruments to be used in commercial transactions." 425 U. S., at 442. 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." *Knotts*, 460 U. S., at 281; see *id.*, at 283 (discussing *Smith*). But when confronted with more pervasive tracking, five Justices agreed that longer term GPS monitoring of even a vehicle traveling on public streets constitutes a search. *Jones*, 565 U. S., at 430 (ALITO, J., concurring in judgment); *id.*, at 415 (SOTOMAYOR, J., concurring). JUSTICE GORSUCH wonders why "someone's location when using a phone" is sensitive, *post,* at 3, and JUSTICE KENNEDY assumes that a person's discrete movements "are not particularly private," *post,* at 17. Yet this 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. *Riley*, 573 U. S., at ___ (slip op., at 9). 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. *Smith*, 442 U. S., at 745.

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 Frankfurter noted when considering new innovations in airplanes and radios, the Court must tread carefully in such cases, to ensure that we do not "embarrass the future." *Northwest Airlines, Inc.* v. *Minnesota*, 322 U. S. 292, 300 (1944).[4]

IV

Having found that the acquisition of Carpenter's CSLI was a search, we also conclude that the Government must generally obtain a warrant supported by probable cause before acquiring such records. Although the "ultimate measure of the constitutionality of a governmental search is 'reasonableness,'" our cases establish that warrantless searches are typically unreasonable where "a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing." *Vernonia School Dist. 47J* v. *Acton*, 515 U. S. 646, 652–653 (1995). Thus, "[i]n the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement." *Riley*, 573 U. S., at ___ (slip op., at 5).

The Government acquired the cell-site records pursuant to a court order issued under the Stored Communications Act, which required the Government to show "reasonable grounds" for believing that the records were "relevant and

---

[4] JUSTICE GORSUCH faults us for not promulgating a complete code addressing the manifold situations that may be presented by this new technology—under a constitutional provision turning on what is "reasonable," no less. *Post,* at 10–12. Like JUSTICE GORSUCH, we "do not begin to claim all the answers today," *post,* at 13, and therefore decide no more than the case before us.

material to an ongoing investigation." 18 U. S. C. §2703(d). That showing falls well short of the probable cause required for a warrant. The Court usually requires "some quantum of individualized suspicion" before a search or seizure may take place. *United States* v. *Martinez-Fuerte*, 428 U. S. 543, 560–561 (1976). Under the standard in the Stored Communications Act, however, law enforcement need only show that the cell-site evidence might be pertinent to an ongoing investigation—a "gigantic" departure from the probable cause rule, as the Government explained below. App. 34. Consequently, an order issued under Section 2703(d) of the Act is not a permissible mechanism for accessing historical cell-site records. Before compelling a wireless carrier to turn over a subscriber's CSLI, the Government's obligation is a familiar one—get a warrant.

JUSTICE ALITO contends that the warrant requirement simply does not apply when the Government acquires records using compulsory process. Unlike an actual search, he says, subpoenas for documents do not involve the direct taking of evidence; they are at most a "constructive search" conducted by the target of the subpoena. *Post,* at 12. Given this lesser intrusion on personal privacy, JUSTICE ALITO argues that the compulsory production of records is not held to the same probable cause standard. In his view, this Court's precedents set forth a categorical rule—separate and distinct from the third-party doctrine—subjecting subpoenas to lenient scrutiny without regard to the suspect's expectation of privacy in the records. *Post,* at 8–19.

But this Court has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy. Almost all of the examples JUSTICE ALITO cites, see *post,* at 14–15, contemplated requests for evidence implicating diminished pri-

vacy interests or for a corporation's own books.[5] The lone exception, of course, is *Miller*, where the Court's analysis of the third-party subpoena merged with the application of the third-party doctrine. 425 U. S., at 444 (concluding that Miller lacked the necessary privacy interest to contest the issuance of a subpoena to his bank).

JUSTICE ALITO overlooks the critical issue. At some point, the dissent should recognize that CSLI is an entirely different species of business record—something that implicates basic Fourth Amendment concerns about arbitrary government power much more directly than corporate tax or payroll ledgers. When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents. See *Riley*, 573 U. S., at ___ (slip op., at 10) ("A search of the information on a cell phone bears little resemblance to the type of brief physical search considered [in prior precedents].").

If the choice to proceed by subpoena provided a categorical limitation on Fourth Amendment protection, no type of record would ever be protected by the warrant requirement. Under JUSTICE ALITO's view, private letters, digital contents of a cell phone—any personal information reduced to document form, in fact—may be collected by

---

[5] See *United States* v. *Dionisio*, 410 U. S. 1, 14 (1973) ("No person can have a reasonable expectation that others will not know the sound of his voice"); *Donovan* v. *Lone Steer, Inc.*, 464 U. S. 408, 411, 415 (1984) (payroll and sales records); *California Bankers Assn.* v. *Shultz*, 416 U. S. 21, 67 (1974) (Bank Secrecy Act reporting requirements); *See* v. *Seattle*, 387 U. S. 541, 544 (1967) (financial books and records); *United States* v. *Powell*, 379 U. S. 48, 49, 57 (1964) (corporate tax records); *McPhaul* v. *United States*, 364 U. S. 372, 374, 382 (1960) (books and records of an organization); *United States* v. *Morton Salt Co.*, 338 U. S. 632, 634, 651–653 (1950) (Federal Trade Commission reporting requirement); *Oklahoma Press Publishing Co.* v. *Walling*, 327 U. S. 186, 189, 204–208 (1946) (payroll records); *Hale* v. *Henkel*, 201 U. S. 43, 45, 75 (1906) (corporate books and papers).

subpoena for no reason other than "official curiosity." *United States* v. *Morton Salt Co.*, 338 U. S. 632, 652 (1950). JUSTICE KENNEDY declines to adopt the radical implications of this theory, leaving open the question whether the warrant requirement applies "when the Government obtains the modern-day equivalents of an individual's own 'papers' or 'effects,' even when those papers or effects are held by a third party." *Post,* at 13 (citing *United States* v. *Warshak*, 631 F. 3d 266, 283–288 (CA6 2010)). That would be a sensible exception, because it would prevent the subpoena doctrine from overcoming any reasonable expectation of privacy. If the third-party doctrine does not apply to the "modern-day equivalents of an individual's own 'papers' or 'effects,'" then the clear implication is that the documents should receive full Fourth Amendment protection. We simply think that such protection should extend as well to a detailed log of a person's movements over several years.

This is certainly not to say that all orders compelling the production of documents will require a showing of probable cause. The Government will be able to use subpoenas to acquire records in the overwhelming majority of investigations. We hold only that a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party.

Further, even though the Government will generally need a warrant to access CSLI, case-specific exceptions may support a warrantless search of an individual's cell-site records under certain circumstances. "One well-recognized exception applies when '"the exigencies of the situation" make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment.'" *Kentucky* v. *King*, 563 U. S. 452, 460 (2011) (quoting *Mincey* v. *Arizona*, 437 U. S. 385, 394 (1978)). Such exigencies include the need to pursue a fleeing suspect, protect individuals who are

threatened with imminent harm, or prevent the imminent destruction of evidence. 563 U. S., at 460, and n. 3.

As a result, if law enforcement is confronted with an urgent situation, such fact-specific threats will likely justify the warrantless collection of CSLI. Lower courts, for instance, have approved warrantless searches related to bomb threats, active shootings, and child abductions. Our decision today does not call into doubt warrantless access to CSLI in such circumstances. While police must get a warrant when collecting CSLI to assist in the mine-run criminal investigation, the rule we set forth does not limit their ability to respond to an ongoing emergency.

* * *

As Justice Brandeis explained in his famous dissent, the Court is obligated—as "[s]ubtler 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 encroachment of the sort the Framers, "after consulting the lessons of history," drafted the Fourth Amendment to prevent. *Di Re*, 332 U. S., at 595.

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.

The judgment of the Court of Appeals is reversed, and

the case is remanded for further proceedings consistent with this opinion.

It is so ordered.

SUPREME COURT OF THE UNITED STATES

No. 16–402

TIMOTHY IVORY CARPENTER, PETITIONER *v.* UNITED STATES

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

[June 22, 2018]

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.

In this case petitioner challenges the Government's right to use compulsory process to obtain a now-common kind of business record: cell-site records held by cell phone service providers. The Government acquired the records through an investigative process enacted by Congress. Upon approval by a neutral magistrate, and based on the Government's duty to show reasonable necessity, it authorizes the disclosure of records and information that are under the control and ownership of the cell phone service provider, not its customer. 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.

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. See *Packingham* v. *North Carolina*, 582 U. S. ___, ___–___ (2017) (slip op., at 4–6). For the reasons that follow, 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.

I

Before evaluating the question presented it is helpful to understand the nature of cell-site records, how they are commonly used by cell phone service providers, and their proper use by law enforcement.

When a cell phone user makes a call, sends a text message or e-mail, or gains access to the Internet, the cell phone establishes a radio connection to an antenna at a nearby cell site. The typical cell site covers a more-or-less

circular geographic area around the site. It has three (or sometimes six) separate antennas pointing in different directions. Each provides cell service for a different 120-degree (or 60-degree) sector of the cell site's circular coverage area. So a cell phone activated on the north side of a cell site will connect to a different antenna than a cell phone on the south side.

Cell phone service providers create records each time a cell phone connects to an antenna at a cell site. For a phone call, for example, the provider records the date, time, and duration of the call; the phone numbers making and receiving the call; and, most relevant here, the cell site used to make the call, as well as the specific antenna that made the connection. The cell-site and antenna data points, together with the date and time of connection, are known as cell-site location information, or cell-site records. By linking an individual's cell phone to a particular 120- or 60-degree sector of a cell site's coverage area at a particular time, cell-site records reveal the general location of the cell phone user.

The location information revealed by cell-site records is imprecise, because an individual cell-site sector usually covers a large geographic area. The FBI agent who offered expert testimony about the cell-site records at issue here testified that a cell site in a city reaches between a half mile and two miles in all directions. That means a 60-degree sector covers between approximately one-eighth and two square miles (and a 120-degree sector twice that area). To put that in perspective, in urban areas cell-site records often would reveal the location of a cell phone user within an area covering between around a dozen and several hundred city blocks. In rural areas cell-site records can be up to 40 times more imprecise. By contrast, a Global Positioning System (GPS) can reveal an individual's location within around 15 feet.

Major cell phone service providers keep cell-site records

for long periods of time. There is no law requiring them to do so. Instead, providers contract with their customers to collect and keep these records because they are valuable to the providers. Among other things, providers aggregate the records and sell them to third parties along with other information gleaned from cell phone usage. This data can be used, for example, to help a department store determine which of various prospective store locations is likely to get more foot traffic from middle-aged women who live in affluent zip codes. The market for cell phone data is now estimated to be in the billions of dollars. See Brief for Technology Experts as *Amici Curiae* 23.

Cell-site records also can serve an important investigative function, as the facts of this case demonstrate. Petitioner, Timothy Carpenter, along with a rotating group of accomplices, robbed at least six RadioShack and T-Mobile stores at gunpoint over a 2-year period. Five of those robberies occurred in the Detroit area, each crime at least four miles from the last. The sixth took place in Warren, Ohio, over 200 miles from Detroit.

The Government, of course, did not know all of these details in 2011 when it began investigating Carpenter. In April of that year police arrested four of Carpenter's co-conspirators. One of them confessed to committing nine robberies in Michigan and Ohio between December 2010 and March 2011. He identified 15 accomplices who had participated in at least one of those robberies; named Carpenter as one of the accomplices; and provided Carpenter's cell phone number to the authorities. The suspect also warned that the other members of the conspiracy planned to commit more armed robberies in the immediate future.

The Government at this point faced a daunting task. Even if it could identify and apprehend the suspects, still it had to link each suspect in this changing criminal gang to specific robberies in order to bring charges and convict.

And, of course, it was urgent that the Government take all necessary steps to stop the ongoing and dangerous crime spree.

Cell-site records were uniquely suited to this task. The geographic dispersion of the robberies meant that, if Carpenter's cell phone were within even a dozen to several hundred city blocks of one or more of the stores when the different robberies occurred, there would be powerful circumstantial evidence of his participation; and this would be especially so if his cell phone usually was not located in the sectors near the stores except during the robbery times.

To obtain these records, the Government applied to federal magistrate judges for disclosure orders pursuant to §2703(d) of the Stored Communications Act. That Act authorizes a magistrate judge to issue an order requiring disclosure of cell-site records if the Government demonstrates "specific and articulable facts showing that there are reasonable grounds to believe" the records "are relevant and material to an ongoing criminal investigation." 18 U. S. C. §§2703(d), 2711(3). The full statutory provision is set out in the Appendix, *infra*.

From Carpenter's primary service provider, MetroPCS, the Government obtained records from between December 2010 and April 2011, based on its understanding that nine robberies had occurred in that timeframe. The Government also requested seven days of cell-site records from Sprint, spanning the time around the robbery in Warren, Ohio. It obtained two days of records.

These records confirmed that Carpenter's cell phone was in the general vicinity of four of the nine robberies, including the one in Ohio, at the times those robberies occurred.

II

The first Clause of the Fourth Amendment provides that "the right of the people to be secure in their persons, houses,

papers, and effects, against unreasonable searches and seizures, shall not be violated." The customary beginning point in any Fourth Amendment search case is whether the Government's actions constitute a "search" of the defendant's person, house, papers, or effects, within the meaning of the constitutional provision. If so, the next question is whether that search was reasonable.

Here the only question necessary to decide is whether the Government searched anything of Carpenter's when it used compulsory process to obtain cell-site records from Carpenter's cell phone service providers. This Court's decisions in *Miller* and *Smith* dictate that the answer is no, as every Court of Appeals to have considered the question has recognized. See *United States* v. *Thompson*, 866 F. 3d 1149 (CA10 2017); *United States* v. *Graham*, 824 F. 3d 421 (CA4 2016) (en banc); *Carpenter* v. *United States*, 819 F. 3d 880 (CA6 2016); *United States* v. *Davis*, 785 F. 3d 498 (CA11 2015) (en banc); *In re Application of U. S. for Historical Cell Site Data*, 724 F. 3d 600 (CA5 2013).

A

Miller and *Smith* hold that individuals lack any protected Fourth Amendment interests in records that are possessed, owned, and controlled only by a third party. In *Miller* federal law enforcement officers obtained four months of the defendant's banking records. 425 U. S., at 437–438. And in *Smith* state police obtained records of the phone numbers dialed from the defendant's home phone. 442 U. S., at 737. The Court held in both cases that the officers did not search anything belonging to the defendants within the meaning of the Fourth Amendment. The defendants could "assert neither ownership nor possession" of the records because the records were created, owned, and controlled by the companies. *Miller*, *supra*, at 440; see *Smith*, *supra*, at 741. And the defendants had no

reasonable expectation of privacy in information they "voluntarily conveyed to the [companies] and exposed to their employees in the ordinary course of business." *Miller*, *supra*, at 442; see *Smith*, 442 U. S., at 744. Rather, the defendants "assumed the risk that the information would be divulged to police." *Id.*, at 745.

Miller and *Smith* have been criticized as being based on too narrow a view of reasonable expectations of privacy. See, *e.g.,* Ashdown, The Fourth Amendment and the "Legitimate Expectation of Privacy," 34 Vand. L. Rev. 1289, 1313–1316 (1981). Those criticisms, however, are unwarranted. The principle established in *Miller* and *Smith* is correct for two reasons, the first relating to a defendant's attenuated interest in property owned by another, and the second relating to the safeguards inherent in the use of compulsory process.

First, *Miller* and *Smith* placed necessary limits on the ability of individuals to assert Fourth Amendment interests in property to which they lack a "requisite connection." *Minnesota* v. *Carter*, 525 U. S. 83, 99 (1998) (KENNEDY, J., concurring). Fourth Amendment rights, after all, are personal. The Amendment protects "[t]he right of the people to be secure in *their* . . . persons, houses, papers, and effects"—not the persons, houses, papers, and effects of others. (Emphasis added.)

The concept of reasonable expectations of privacy, first announced in *Katz* v. *United States*, 389 U. S. 347 (1967), sought to look beyond the "arcane distinctions developed in property and tort law" in evaluating whether a person has a sufficient connection to the thing or place searched to assert Fourth Amendment interests in it. *Rakas* v. *Illinois*, 439 U. S. 128, 143 (1978). Yet "property concepts" are, nonetheless, fundamental "in determining the presence or absence of the privacy interests protected by that Amendment." *Id.,* at 143–144, n. 12. This is so for at least two reasons. First, as a matter of settled expectations

from the law of property, individuals often have greater expectations of privacy in things and places that belong to them, not to others. And second, the Fourth Amendment's protections must remain tethered to the text of that Amendment, which, again, protects only a person's own "persons, houses, papers, and effects."

Katz did not abandon reliance on property-based concepts. The Court in *Katz* analogized the phone booth used in that case to a friend's apartment, a taxicab, and a hotel room. 389 U. S., at 352, 359. So when the defendant "shu[t] the door behind him" and "pa[id] the toll," *id.,* at 352, he had a temporary interest in the space and a legitimate expectation that others would not intrude, much like the interest a hotel guest has in a hotel room, *Stoner* v. *California*, 376 U. S. 483 (1964), or an overnight guest has in a host's home, *Minnesota* v. *Olson*, 495 U. S. 91 (1990). The Government intruded on that space when it attached a listening device to the phone booth. *Katz*, 389 U. S., at 348. (And even so, the Court made it clear that the Government's search could have been reasonable had there been judicial approval on a case-specific basis, which, of course, did occur here. *Id*., at 357–359.)

Miller and *Smith* set forth an important and necessary limitation on the *Katz* framework. They rest upon the commonsense principle that the absence of property law analogues can be dispositive of privacy expectations. The defendants in those cases could expect that the third-party businesses could use the records the companies collected, stored, and classified as their own for any number of business and commercial purposes. The businesses were not bailees or custodians of the records, with a duty to hold the records for the defendants' use. The defendants could make no argument that the records were their own papers or effects. See *Miller*, *supra*, at 440 ("the documents subpoenaed here are not respondent's 'private papers'"); *Smith*, *supra*, at 741 ("petitioner obviously

cannot claim that his 'property' was invaded"). The records were the business entities' records, plain and simple. The defendants had no reason to believe the records were owned or controlled by them and so could not assert a reasonable expectation of privacy in the records.

The second principle supporting *Miller* and *Smith* is the longstanding rule that the Government may use compulsory process to compel persons to disclose documents and other evidence within their possession and control. See *United States* v. *Nixon*, 418 U. S. 683, 709 (1974) (it is an "ancient proposition of law" that "the public has a right to every man's evidence" (internal quotation marks and alterations omitted)). A subpoena is different from a warrant in its force and intrusive power. While a warrant allows the Government to enter and seize and make the examination itself, a subpoena simply requires the person to whom it is directed to make the disclosure. A subpoena, moreover, provides the recipient the "opportunity to present objections" before complying, which further mitigates the intrusion. *Oklahoma Press Publishing Co.* v. *Walling*, 327 U. S. 186, 195 (1946).

For those reasons this Court has held that a subpoena for records, although a "constructive" search subject to Fourth Amendment constraints, need not comply with the procedures applicable to warrants—even when challenged by the person to whom the records belong. *Id.,* at 202, 208. Rather, a subpoena complies with the Fourth Amendment's reasonableness requirement so long as it is "'sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome.'" *Donovan* v. *Lone Steer, Inc.*, 464 U. S. 408, 415 (1984). Persons with no meaningful interests in the records sought by a subpoena, like the defendants in *Miller* and *Smith*, have no rights to object to the records' disclosure—much less to assert that the Government must obtain a warrant to compel disclosure of the

records. See *Miller*, 425 U. S., at 444–446; *SEC* v. *Jerry T. O'Brien, Inc.*, 467 U. S. 735, 742–743 (1984).

Based on *Miller* and *Smith* and the principles underlying those cases, it is well established that subpoenas may be used to obtain a wide variety of records held by businesses, even when the records contain private information. See 2 W. LaFave, Search and Seizure §4.13 (5th ed. 2012). Credit cards are a prime example. State and federal law enforcement, for instance, often subpoena credit card statements to develop probable cause to prosecute crimes ranging from drug trafficking and distribution to healthcare fraud to tax evasion. See *United States* v. *Phibbs*, 999 F. 2d 1053 (CA6 1993) (drug distribution); *McCune* v. *DOJ*, 592 Fed. Appx. 287 (CA5 2014) (healthcare fraud); *United States* v. *Green*, 305 F. 3d 422 (CA6 2002) (drug trafficking and tax evasion); see also 12 U. S. C. §§3402(4), 3407 (allowing the Government to subpoena financial records if "there is reason to believe that the records sought are relevant to a legitimate law enforcement inquiry"). Subpoenas also may be used to obtain vehicle registration records, hotel records, employment records, and records of utility usage, to name just a few other examples. See 1 LaFave, *supra*, §2.7(c).

And law enforcement officers are not alone in their reliance on subpoenas to obtain business records for legitimate investigations. Subpoenas also are used for investigatory purposes by state and federal grand juries, see *United States* v. *Dionisio*, 410 U. S. 1 (1973), state and federal administrative agencies, see *Oklahoma Press*, *supra*, and state and federal legislative bodies, see *McPhaul* v. *United States*, 364 U. S. 372 (1960).

B

Carpenter does not question these traditional investigative practices. And he does not ask the Court to reconsider *Miller* and *Smith*. Carpenter argues only that, under

Miller and *Smith*, the Government may not use compulsory process to acquire cell-site records from cell phone service providers.

There is no merit in this argument. Cell-site records, like all the examples just discussed, are created, kept, classified, owned, and controlled by cell phone service providers, which aggregate and sell this information to third parties. As in *Miller*, Carpenter can "assert neither ownership nor possession" of the records and has no control over them. 425 U. S., at 440.

Carpenter argues that he has Fourth Amendment interests in the cell-site records because they are in essence his personal papers by operation of 47 U. S. C. §222. That statute imposes certain restrictions on how providers may use "customer proprietary network information"—a term that encompasses cell-site records. §§222(c), (h)(1)(A). The statute in general prohibits providers from disclosing personally identifiable cell-site records to private third parties. §222(c)(1). And it allows customers to request cell-site records from the provider. §222(c)(2).

Carpenter's argument is unpersuasive, however, for §222 does not grant cell phone customers any meaningful interest in cell-site records. The statute's confidentiality protections may be overridden by the interests of the providers or the Government. The providers may disclose the records "to protect the[ir] rights or property" or to "initiate, render, bill, and collect for telecommunications services." §§222(d)(1), (2). They also may disclose the records "as required by law"—which, of course, is how they were disclosed in this case. §222(c)(1). Nor does the statute provide customers any practical control over the records. Customers do not create the records; they have no say in whether or for how long the records are stored; and they cannot require the records to be modified or destroyed. Even their right to request access to the records is limited, for the statute "does not preclude a carrier from

being reimbursed by the customers . . . for the costs associated with making such disclosures." H. R. Rep. No. 104–204, pt. 1, p. 90 (1995). So in every legal and practical sense the "network information" regulated by §222 is, under that statute, "proprietary" to the service providers, not Carpenter. The Court does not argue otherwise.

Because Carpenter lacks a requisite connection to the cell-site records, he also may not claim a reasonable expectation of privacy in them. He could expect that a third party—the cell phone service provider—could use the information it collected, stored, and classified as its own for a variety of business and commercial purposes.

All this is not to say that *Miller* and *Smith* are without limits. *Miller* and *Smith* may not apply when the Government obtains the modern-day equivalents of an individual's own "papers" or "effects," even when those papers or effects are held by a third party. See *Ex parte Jackson*, 96 U. S. 727, 733 (1878) (letters held by mail carrier); *United States* v. *Warshak*, 631 F. 3d 266, 283–288 (CA6 2010) (e-mails held by Internet service provider). As already discussed, however, this case does not involve property or a bailment of that sort. Here the Government's acquisition of cell-site records falls within the heartland of *Miller* and *Smith*.

In fact, Carpenter's Fourth Amendment objection is even weaker than those of the defendants in *Miller* and *Smith*. Here the Government did not use a mere subpoena to obtain the cell-site records. It acquired the records only after it proved to a Magistrate Judge reasonable grounds to believe that the records were relevant and material to an ongoing criminal investigation. See 18 U. S. C. §2703(d). So even if §222 gave Carpenter some attenuated interest in the records, the Government's conduct here would be reasonable under the standards governing subpoenas. See *Donovan*, 464 U. S., at 415.

Under *Miller* and *Smith*, then, a search of the sort that

requires a warrant simply did not occur when the Government used court-approved compulsory process, based on a finding of reasonable necessity, to compel a cell phone service provider, as owner, to disclose cell-site records.

III

The Court rejects a straightforward application of *Miller* and *Smith*. It concludes instead that applying those cases to cell-site records would work a "significant extension" of the principles underlying them, *ante,* at 15, and holds that the acquisition of more than six days of cell-site records constitutes a search, *ante,* at 11, n. 3.

In my respectful view the majority opinion misreads this Court's precedents, old and recent, and transforms *Miller* and *Smith* into an unprincipled and unworkable doctrine. The Court's newly conceived constitutional standard will cause confusion; will undermine traditional and important law enforcement practices; and will allow the cell phone to become a protected medium that dangerous persons will use to commit serious crimes.

A

The Court errs at the outset by attempting to sidestep *Miller* and *Smith*. The Court frames this case as following instead from *United States* v. *Knotts*, 460 U. S. 276 (1983), and *United States* v. *Jones*, 565 U. S. 400 (2012). Those cases, the Court suggests, establish that "individuals have a reasonable expectation of privacy in the whole of their physical movements." *Ante*, at 7–9, 12.

Knotts held just the opposite: "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." 460 U. S., at 281. True, the Court in *Knotts* also suggested that "different constitutional principles may be applicable" to "dragnet-type law enforcement practices." *Id.,* at 284. But by dragnet practices the Court was refer-

ring to "'twenty-four hour surveillance of any citizen of this country . . . without judicial knowledge or supervision.'" *Id.*, at 283.

Those "different constitutional principles" mentioned in *Knotts*, whatever they may be, do not apply in this case. Here the Stored Communications Act requires a neutral judicial officer to confirm in each case that the Government has "reasonable grounds to believe" the cell-site records "are relevant and material to an ongoing criminal investigation." 18 U. S. C. §2703(d). This judicial check mitigates the Court's concerns about "'a too permeating police surveillance.'" *Ante*, at 6 (quoting *United States* v. *Di Re*, 332 U. S. 581, 595 (1948)). Here, even more so than in *Knotts*, "reality hardly suggests abuse." 460 U. S., at 284.

The Court's reliance on *Jones* fares no better. In *Jones* the Government installed a GPS tracking device on the defendant's automobile. The Court held the Government searched the automobile because it "physically occupied private property [of the defendant] for the purpose of obtaining information." 565 U. S., at 404. So in *Jones* it was "not necessary to inquire about the target's expectation of privacy in his vehicle's movements." *Grady* v. *North Carolina*, 575 U. S. ___, ___ (2015) (*per curiam*) (slip op., at 3).

Despite that clear delineation of the Court's holding in *Jones*, the Court today declares that *Jones* applied the "'different constitutional principles'" alluded to in *Knotts* to establish that an individual has an expectation of privacy in the sum of his whereabouts. *Ante*, at 8, 12. For that proposition the majority relies on the two concurring opinions in *Jones*, one of which stated that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." 565 U. S., at 430 (ALITO, J., concurring). But *Jones* involved direct governmental surveillance of a defendant's automobile without judicial

authorization—specifically, GPS surveillance accurate within 50 to 100 feet. *Id.*, at 402–403. Even assuming that the different constitutional principles mentioned in *Knotts* would apply in a case like *Jones*—a proposition the Court was careful not to announce in *Jones*, *supra*, at 412–413—those principles are inapplicable here. Cases like this one, where the Government uses court-approved compulsory process to obtain records owned and controlled by a third party, are governed by the two majority opinions in *Miller* and *Smith*.

B

The Court continues its analysis by misinterpreting *Miller* and *Smith*, and then it reaches the wrong outcome on these facts even under its flawed standard.

The Court appears, in my respectful view, to read *Miller* and *Smith* to establish a balancing test. For each "qualitatively different category" of information, the Court suggests, the privacy interests at stake must be weighed against the fact that the information has been disclosed to a third party. See *ante*, at 11, 15–17. When the privacy interests are weighty enough to "overcome" the third-party disclosure, the Fourth Amendment's protections apply. See *ante*, at 17.

That is an untenable reading of *Miller* and *Smith*. As already discussed, the fact that information was relinquished to a third party was the entire basis for concluding that the defendants in those cases lacked a reasonable expectation of privacy. *Miller* and *Smith* do not establish the kind of category-by-category balancing the Court today prescribes.

But suppose the Court were correct to say that *Miller* and *Smith* rest on so imprecise a foundation. Still the Court errs, in my submission, when it concludes that cell-site records implicate greater privacy interests—and thus deserve greater Fourth Amendment protection—than

financial records and telephone records.

Indeed, the opposite is true. A person's movements are not particularly private. As the Court recognized in *Knotts*, when the defendant there "traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination." 460 U. S., at 281–282. Today expectations of privacy in one's location are, if anything, even less reasonable than when the Court decided *Knotts* over 30 years ago. Millions of Americans choose to share their location on a daily basis, whether by using a variety of location-based services on their phones, or by sharing their location with friends and the public at large via social media.

And cell-site records, as already discussed, disclose a person's location only in a general area. The records at issue here, for example, revealed Carpenter's location within an area covering between around a dozen and several hundred city blocks. "Areas of this scale might encompass bridal stores and Bass Pro Shops, gay bars and straight ones, a Methodist church and the local mosque." 819 F. 3d 880, 889 (CA6 2016). These records could not reveal where Carpenter lives and works, much less his "'familial, political, professional, religious, and sexual associations.'" *Ante*, at 12 (quoting *Jones*, *supra*, at 415 (SOTOMAYOR, J., concurring)).

By contrast, financial records and telephone records do "'revea[l] . . . personal affairs, opinions, habits and associations.'" *Miller*, 425 U. S., at 451 (Brennan, J., dissenting); see *Smith*, 442 U. S., at 751 (Marshall, J., dissenting). What persons purchase and to whom they talk might disclose how much money they make; the political and religious organizations to which they donate; whether they have visited a psychiatrist, plastic surgeon, abortion clinic, or AIDS treatment center; whether they go to gay bars or

straight ones; and who are their closest friends and family members. The troves of intimate information the Government can and does obtain using financial records and telephone records dwarfs what can be gathered from cell-site records.

Still, the Court maintains, cell-site records are "unique" because they are "comprehensive" in their reach; allow for retrospective collection; are "easy, cheap, and efficient compared to traditional investigative tools"; and are not exposed to cell phone service providers in a meaningfully voluntary manner. *Ante*, at 11–13, 17, 22. But many other kinds of business records can be so described. Financial records are of vast scope. Banks and credit card companies keep a comprehensive account of almost every transaction an individual makes on a daily basis. "With just the click of a button, the Government can access each [company's] deep repository of historical [financial] information at practically no expense." *Ante*, at 12–13. And the decision whether to transact with banks and credit card companies is no more or less voluntary than the decision whether to use a cell phone. Today, just as when *Miller* was decided, "'it is impossible to participate in the economic life of contemporary society without maintaining a bank account.'" 425 U. S., at 451 (Brennan, J., dissenting). But this Court, nevertheless, has held that individuals do not have a reasonable expectation of privacy in financial records.

Perhaps recognizing the difficulty of drawing the constitutional line between cell-site records and financial and telephonic records, the Court posits that the accuracy of cell-site records "is rapidly approaching GPS-level precision." *Ante*, at 14. That is certainly plausible in the era of cyber technology, yet the privacy interests associated with location information, which is often disclosed to the public at large, still would not outweigh the privacy interests implicated by financial and telephonic records.

Perhaps more important, those future developments are no basis upon which to resolve this case. In general, the Court "risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." *Ontario* v. *Quon*, 560 U. S. 746, 759 (2010). That judicial caution, prudent in most cases, is imperative in this one.

Technological changes involving cell phones have complex effects on crime and law enforcement. Cell phones make crimes easier to coordinate and conceal, while also providing the Government with new investigative tools that may have the potential to upset traditional privacy expectations. See Kerr, An Equilibrium-Adjustment Theory of the Fourth Amendment, 125 Harv. L. Rev 476, 512–517 (2011). How those competing effects balance against each other, and how property norms and expectations of privacy form around new technology, often will be difficult to determine during periods of rapid technological change. In those instances, and where the governing legal standard is one of reasonableness, it is wise to defer to legislative judgments like the one embodied in §2703(d) of the Stored Communications Act. See *Jones*, 565 U. S., at 430 (ALITO, J., concurring). In §2703(d) Congress weighed the privacy interests at stake and imposed a judicial check to prevent executive overreach. The Court should be wary of upsetting that legislative balance and erecting constitutional barriers that foreclose further legislative instructions. See *Quon*, *supra*, at 759. The last thing the Court should do is incorporate an arbitrary and outside limit—in this case six days' worth of cell-site records—and use it as the foundation for a new constitutional framework. The Court's decision runs roughshod over the mechanism Congress put in place to govern the acquisition of cell-site records and closes off further legislative debate on these issues.

C

The Court says its decision is a "narrow one." *Ante,* at 17. But its reinterpretation of *Miller* and *Smith* will have dramatic consequences for law enforcement, courts, and society as a whole.

Most immediately, the Court's holding that the Government must get a warrant to obtain more than six days of cell-site records limits the effectiveness of an important investigative tool for solving serious crimes. As this case demonstrates, cell-site records are uniquely suited to help the Government develop probable cause to apprehend some of the Nation's most dangerous criminals: serial killers, rapists, arsonists, robbers, and so forth. See also, *e.g.*, *Davis*, 785 F. 3d, at 500–501 (armed robbers); Brief for Alabama et al. as *Amici Curiae* 21–22 (serial killer). These records often are indispensable at the initial stages of investigations when the Government lacks the evidence necessary to obtain a warrant. See *United States* v. *Pembrook*, 876 F. 3d 812, 816–819 (CA6 2017). And the long-term nature of many serious crimes, including serial crimes and terrorism offenses, can necessitate the use of significantly more than six days of cell-site records. The Court's arbitrary 6-day cutoff has the perverse effect of nullifying Congress' reasonable framework for obtaining cell-site records in some of the most serious criminal investigations.

The Court's decision also will have ramifications that extend beyond cell-site records to other kinds of information held by third parties, yet the Court fails "to provide clear guidance to law enforcement" and courts on key issues raised by its reinterpretation of *Miller* and *Smith*. *Riley* v. *California*, 573 U. S. ___, ___ (2014) (slip op., at 22).

First, the Court's holding is premised on cell-site records being a "distinct category of information" from other busi-

ness records. *Ante*, at 15. But the Court does not explain what makes something a distinct category of information. Whether credit card records are distinct from bank records; whether payment records from digital wallet applications are distinct from either; whether the electronic bank records available today are distinct from the paper and microfilm records at issue in *Miller*; or whether cell-phone call records are distinct from the home-phone call records at issue in *Smith*, are just a few of the difficult questions that require answers under the Court's novel conception of *Miller* and *Smith*.

Second, the majority opinion gives courts and law enforcement officers no indication how to determine whether any particular category of information falls on the financial-records side or the cell-site-records side of its newly conceived constitutional line. The Court's multifactor analysis—considering intimacy, comprehensiveness, expense, retrospectivity, and voluntariness—puts the law on a new and unstable foundation.

Third, even if a distinct category of information is deemed to be more like cell-site records than financial records, courts and law enforcement officers will have to guess how much of that information can be requested before a warrant is required. The Court suggests that less than seven days of location information may not require a warrant. See *ante,* at 11, n. 3; see also *ante,* at 17–18 (expressing no opinion on "real-time CSLI," tower dumps, and security-camera footage). But the Court does not explain why that is so, and nothing in its opinion even alludes to the considerations that should determine whether greater or lesser thresholds should apply to information like IP addresses or website browsing history.

Fourth, by invalidating the Government's use of court-approved compulsory process in this case, the Court calls into question the subpoena practices of federal and state grand juries, legislatures, and other investigative bodies,

as JUSTICE ALITO's opinion explains. See *post,* at 2–19 (dissenting opinion). Yet the Court fails even to mention the serious consequences this will have for the proper administration of justice.

In short, the Court's new and uncharted course will inhibit law enforcement and "keep defendants and judges guessing for years to come." *Riley*, 573 U. S., at ___ (slip op., at 25) (internal quotation marks omitted).

* * *

This case should be resolved by interpreting accepted property principles as the baseline for reasonable expectations of privacy. Here the Government did not search anything over which Carpenter could assert ownership or control. Instead, it issued a court-authorized subpoena to a third party to disclose information it alone owned and controlled. That should suffice to resolve this case.

Having concluded, however, that the Government searched Carpenter when it obtained cell-site records from his cell phone service providers, the proper resolution of this case should have been to remand for the Court of Appeals to determine in the first instance whether the search was reasonable. Most courts of appeals, believing themselves bound by *Miller* and *Smith*, have not grappled with this question. And the Court's reflexive imposition of the warrant requirement obscures important and difficult issues, such as the scope of Congress' power to authorize the Government to collect new forms of information using processes that deviate from traditional warrant procedures, and how the Fourth Amendment's reasonableness requirement should apply when the Government uses compulsory process instead of engaging in an actual, physical search.

These reasons all lead to this respectful dissent.

APPENDIX

"**§2703. Required disclosure of customer communications or records**

"(d) REQUIREMENTS FOR COURT ORDER.—A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider."

SUPREME COURT OF THE UNITED STATES

No. 16–402

TIMOTHY IVORY CARPENTER, PETITIONER *v.* UNITED STATES

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

[June 22, 2018]

JUSTICE THOMAS, dissenting.

This case should not turn on "whether" a search occurred. *Ante,* at 1. It should turn, instead, on *whose* property was searched. The Fourth Amendment guarantees individuals the right to be secure from unreasonable searches of "*their* persons, houses, papers, and effects." (Emphasis added.) In other words, "*each* person has the right to be secure against unreasonable searches . . . in *his own* person, house, papers, and effects." *Minnesota* v. *Carter*, 525 U. S. 83, 92 (1998) (Scalia, J., concurring). By obtaining the cell-site records of MetroPCS and Sprint, the Government did not search Carpenter's property. He did not create the records, he does not maintain them, he cannot control them, and he cannot destroy them. Neither the terms of his contracts nor any provision of law makes the records his. The records belong to MetroPCS and Sprint.

The Court concludes that, although the records are not Carpenter's, the Government must get a warrant because Carpenter had a reasonable "expectation of privacy" in the location information that they reveal. *Ante,* at 11. I agree with JUSTICE KENNEDY, JUSTICE ALITO, JUSTICE GORSUCH, and every Court of Appeals to consider the question that this is not the best reading of our precedents.

The more fundamental problem with the Court's opinion, however, is its use of the "reasonable expectation of privacy" test, which was first articulated by Justice Harlan in *Katz* v. *United States*, 389 U. S. 347, 360–361 (1967) (concurring opinion). The *Katz* test has no basis in the text or history of the Fourth Amendment. And, it invites courts to make judgments about policy, not law. Until we confront the problems with this test, *Katz* will continue to distort Fourth Amendment jurisprudence. I respectfully dissent.

I

Katz was the culmination of a series of decisions applying the Fourth Amendment to electronic eavesdropping. The first such decision was *Olmstead* v. *United States*, 277 U. S. 438 (1928), where federal officers had intercepted the defendants' conversations by tapping telephone lines near their homes. *Id.,* at 456–457. In an opinion by Chief Justice Taft, the Court concluded that this wiretap did not violate the Fourth Amendment. No "search" occurred, according to the Court, because the officers did not physically enter the defendants' homes. *Id.,* at 464–466. And neither the telephone lines nor the defendants' intangible conversations qualified as "persons, houses, papers, [or] effects" within the meaning of the Fourth Amendment. *Ibid.*[1] In the ensuing decades, this Court adhered to

---

[1]Justice Brandeis authored the principal dissent in *Olmstead*. He consulted the "underlying purpose," rather than "the words of the [Fourth] Amendment," to conclude that the wiretap was a search. 277 U. S., at 476. In Justice Brandeis' view, the Framers "recognized the significance of man's spiritual nature, of his feelings and of his intellect" and "sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations." *Id.,* at 478. Thus, "every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed," should constitute an unreasonable search under the Fourth Amendment. *Ibid.*

Olmstead and rejected Fourth Amendment challenges to various methods of electronic surveillance. See *On Lee* v. *United States*, 343 U. S. 747, 749–753 (1952) (use of microphone to overhear conversations with confidential informant); *Goldman* v. *United States*, 316 U. S. 129, 131–132, 135–136 (1942) (use of detectaphone to hear conversations in office next door).

In the 1960's, however, the Court began to retreat from *Olmstead*. In *Silverman* v. *United States*, 365 U. S. 505 (1961), for example, federal officers had eavesdropped on the defendants by driving a "spike mike" several inches into the house they were occupying. *Id.,* at 506–507. This was a "search," the Court held, because the "unauthorized physical penetration into the premises" was an "actual intrusion into a constitutionally protected area." *Id.,* at 509, 512. The Court did not mention *Olmstead*'s other holding that intangible conversations are not "persons, houses, papers, [or] effects." That omission was significant. The Court confirmed two years later that "[i]t follows from [*Silverman*] that the Fourth Amendment may protect against the overhearing of verbal statements as well as against the more traditional seizure of 'papers and effects.'" *Wong Sun* v. *United States*, 371 U. S. 471, 485 (1963); accord, *Berger* v. *New York*, 388 U. S. 41, 51 (1967).

In *Katz*, the Court rejected *Olmstead*'s remaining holding—that eavesdropping is not a search absent a physical intrusion into a constitutionally protected area. The federal officers in *Katz* had intercepted the defendant's conversations by attaching an electronic device to the outside of a public telephone booth. 389 U. S., at 348. The Court concluded that this was a "search" because the officers "violated the privacy upon which [the defendant] justifiably relied while using the telephone booth." *Id.,* at 353. Although the device did not physically penetrate the booth, the Court overruled *Olmstead* and held that "the reach of [the Fourth] Amendment cannot turn upon the

presence or absence of a physical intrusion." 389 U. S., at 353. The Court did not explain what should replace *Olmstead*'s physical-intrusion requirement. It simply asserted that "the Fourth Amendment protects people, not places" and "what [a person] seeks to preserve as private . . . may be constitutionally protected." 389 U. S., at 351.

Justice Harlan's concurrence in *Katz* attempted to articulate the standard that was missing from the majority opinion. While Justice Harlan agreed that "'the Fourth Amendment protects people, not places,'" he stressed that "[t]he question . . . is what protection it affords to those people," and "the answer . . . requires reference to a 'place.'" *Id.,* at 361. Justice Harlan identified a "twofold requirement" to determine when the protections of the Fourth Amendment apply: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Ibid.*

Justice Harlan did not cite anything for this "expectation of privacy" test, and the parties did not discuss it in their briefs. The test appears to have been presented for the first time at oral argument by one of the defendant's lawyers. See Winn, *Katz* and the Origins of the "Reasonable Expectation of Privacy" Test, 40 McGeorge L. Rev. 1, 9–10 (2009). The lawyer, a recent law-school graduate, apparently had an "[e]piphany" while preparing for oral argument. Schneider, *Katz v. United States*: The Untold Story, 40 McGeorge L. Rev. 13, 18 (2009). He conjectured that, like the "reasonable person" test from his Torts class, the Fourth Amendment should turn on "whether a reasonable person . . . could have expected his communication to be private." *Id.,* at 19. The lawyer presented his new theory to the Court at oral argument. See, *e.g.,* Tr. of Oral Arg. in *Katz* v. *United States*, O. T. 1967, No. 35, p. 5 (proposing a test of "whether or not, objectively speaking, the communication was intended to be private"); *id.,* at 11

("We propose a test using a way that's not too dissimilar from the tort 'reasonable man' test"). After some questioning from the Justices, the lawyer conceded that his test should also require individuals to subjectively expect privacy. See *id.,* at 12. With that modification, Justice Harlan seemed to accept the lawyer's test almost verbatim in his concurrence.

Although the majority opinion in *Katz* had little practical significance after Congress enacted the Omnibus Crime Control and Safe Streets Act of 1968, Justice Harlan's concurrence profoundly changed our Fourth Amendment jurisprudence. It took only one year for the full Court to adopt his two-pronged test. See *Terry* v. *Ohio*, 392 U. S. 1, 10 (1968). And by 1979, the Court was describing Justice Harlan's test as the "lodestar" for determining whether a "search" had occurred. *Smith* v. *Maryland*, 442 U. S. 735, 739 (1979). Over time, the Court minimized the subjective prong of Justice Harlan's test. See Kerr, *Katz* Has Only One Step: The Irrelevance of Subjective Expectations, 82 U. Chi. L. Rev. 113 (2015). That left the objective prong—the "reasonable expectation of privacy" test that the Court still applies today. See *ante,* at 5; *United States* v. *Jones*, 565 U. S. 400, 406 (2012).

II

Under the *Katz* test, a "search" occurs whenever "government officers violate a person's 'reasonable expectation of privacy.'" *Jones*, *supra,* at 406. The most glaring problem with this test is that it has "no plausible foundation in the text of the Fourth Amendment." *Carter*, 525 U. S., at 97 (opinion of Scalia, J.). The Fourth Amendment, as relevant here, protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches." By defining "search" to mean "any violation of a reasonable expectation of pri-

vacy," the *Katz* test misconstrues virtually every one of these words.

A

The *Katz* test distorts the original meaning of "searc[h]"—the word in the Fourth Amendment that it purports to define, see *ante*, at 5; *Smith*, *supra*. Under the *Katz* test, the government conducts a search anytime it violates someone's "reasonable expectation of privacy." That is not a normal definition of the word "search."

At the founding, "search" did not mean a violation of someone's reasonable expectation of privacy. The word was probably not a term of art, as it does not appear in legal dictionaries from the era. And its ordinary meaning was the same as it is today: "'[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as, to *search* the house for a book; to *search* the wood for a thief.'" *Kyllo* v. *United States*, 533 U. S. 27, 32, n. 1 (2001) (quoting N. Webster, An American Dictionary of the English Language 66 (1828) (reprint 6th ed. 1989)); accord, 2 S. Johnson, A Dictionary of the English Language (5th ed. 1773) ("Inquiry by looking into every suspected place"); N. Bailey, An Universal Etymological English Dictionary (22d ed. 1770) ("a seeking after, a looking for, &c."); 2 J. Ash, The New and Complete Dictionary of the English Language (2d ed. 1795) ("An enquiry, an examination, the act of seeking, an enquiry by looking into every suspected place; a quest; a pursuit"); T. Sheridan, A Complete Dictionary of the English Language (6th ed. 1796) (similar). The word "search" was not associated with "reasonable expectation of privacy" until Justice Harlan coined that phrase in 1967. The phrase "expectation(s) of privacy" does not appear in the pre-*Katz* federal or state case reporters, the papers of prominent

Founders,[2] early congressional documents and debates,[3] collections of early American English texts,[4] or early American newspapers.[5]

B

The *Katz* test strays even further from the text by focusing on the concept of "privacy." The word "privacy" does not appear in the Fourth Amendment (or anywhere else in the Constitution for that matter). Instead, the Fourth Amendment references "[t]he right of the people to be secure." It then qualifies that right by limiting it to "persons" and three specific types of property: "houses, papers, and effects." By connecting the right to be secure to these four specific objects, "[t]he text of the Fourth Amendment reflects its close connection to property." *Jones*, *supra*, at 405. "[P]rivacy," by contrast, "was not part of the political vocabulary of the [founding]. Instead, liberty and privacy rights were understood largely in terms of property rights." Cloud, Property Is Privacy: Locke and Brandeis in the Twenty-First Century, 55 Am. Crim. L. Rev. 37, 42 (2018).

Those who ratified the Fourth Amendment were quite familiar with the notion of security in property. Security in property was a prominent concept in English law. See, *e.g.,* 3 W. Blackstone, Commentaries on the Laws of Eng-

---

[2] National Archives, Library of Congress, Founders Online, https://founders.archives.gov (all Internet materials as last visited June 18, 2018).

[3] A Century of Lawmaking For A New Nation, U. S. Congressional Documents and Debates, 1774–1875 (May 1, 2003), https://memory.loc.gov/ammem/amlaw/lawhome.html.

[4] Corpus of Historical American English, https://corpus.byu.edu/coha; Google Books (American), https://googlebooks.byu.edu/x.asp; Corpus of Founding Era American English, https://lawncl.byu.edu/cofea.

[5] Readex, America's Historical Newspapers (2018), https://www.readex.com/content/americas-historical-newspapers.

land 288 (1768) ("[E]very man's house is looked upon by the law to be his castle"); 3 E. Coke, Institutes of Laws of England 162 (6th ed. 1680) ("[F]or a man[']s house is his Castle, & domus sua cuique est tutissimum refugium [each man's home is his safest refuge]"). The political philosophy of John Locke, moreover, "permeated the 18th-century political scene in America." *Obergefell* v. *Hodges*, 576 U. S. ___, ___ (2015) (THOMAS, J., dissenting) (slip op., at 8). For Locke, every individual had a property right "in his own person" and in anything he "removed from the common state [of] Nature" and "mixed his labour with." Second Treatise of Civil Government §27 (1690). Because property is "very unsecure" in the state of nature, §123, individuals form governments to obtain "a secure enjoyment of their properties." §95. Once a government is formed, however, it cannot be given "a power to destroy that which every one designs to secure"; it cannot legitimately "endeavour to take away, and destroy the property of the people," or exercise "an absolute power over [their] lives, liberties, and estates." §222.

The concept of security in property recognized by Locke and the English legal tradition appeared throughout the materials that inspired the Fourth Amendment. In *Entick* v. *Carrington*, 19 How. St. Tr. 1029 (C. P. 1765)—a heralded decision that the founding generation considered "the true and ultimate expression of constitutional law," *Boyd* v. *United States*, 116 U. S. 616, 626 (1886)—Lord Camden explained that "[t]he great end, for which men entered into society, was to secure their property." 19 How. St. Tr., at 1066. The American colonists echoed this reasoning in their "widespread hostility" to the Crown's writs of assistance[6]—a practice that inspired the Revolu-

[6] Writs of assistance were "general warrants" that gave "customs officials blanket authority to search where they pleased for goods

tion and became "[t]he driving force behind the adoption of the [Fourth] Amendment." *United States* v. *Verdugo-Urquidez*, 494 U. S. 259, 266 (1990). Prominent colonists decried the writs as destroying "'domestic security'" by permitting broad searches of homes. M. Smith, The Writs of Assistance Case 475 (1978) (quoting a 1772 Boston town meeting); see also *id.,* at 562 (complaining that "'every householder in this province, will necessarily become *less secure* than he was before this writ'" (quoting a 1762 article in the Boston Gazette)); *id.,* at 493 (complaining that the writs were "'expressly contrary to the common law, which ever regarded a man's *house* as his castle, or a place of perfect security'" (quoting a 1768 letter from John Dickinson)). John Otis, who argued the famous Writs of Assistance case, contended that the writs violated "'the fundamental Principl[e] of Law'" that "'[a] Man who is quiet, is as secure in his House, as a Prince in his Castle.'" *Id.,* at 339 (quoting John Adam's notes). John Adams attended Otis' argument and later drafted Article XIV of the Massachusetts Constitution,[7] which served as a model for the Fourth Amendment. See Clancy, The Framers' Intent: John Adams, His Era, and the Fourth Amendment, 86 Ind. L. J. 979, 982 (2011); Donahue, The Original Fourth Amendment, 83 U. Chi. L. Rev. 1181, 1269 (2016)

---

imported in violation of the British tax laws." *Stanford* v. *Texas*, 379 U. S. 476, 481 (1965).

[7] "Every subject has a right to be secure from all unreasonable searches and seizures of his person, his house, his papers, and all his possessions. All warrants, therefore, are contrary to right, if the cause or foundation of them be not previously supported by oath or affirmation, and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the person or objects of search, arrest, or seizure; and no warrant ought to be issued but in cases, and with the formalities prescribed by the laws." Mass. Const., pt. I, Art. XIV (1780).

(Donahue). Adams agreed that "[p]roperty must be secured, or liberty cannot exist." Discourse on Davila, in 6 The Works of John Adams 280 (C. Adams ed. 1851).

Of course, the founding generation understood that, by securing their property, the Fourth Amendment would often protect their privacy as well. See, *e.g., Boyd*, *supra*, at 630 (explaining that searches of houses invade "the privacies of life"); *Wilkes* v. *Wood*, 19 How. St. Tr. 1153, 1154 (C. P. 1763) (argument of counsel contending that seizures of papers implicate "our most private concerns"). But the Fourth Amendment's attendant protection of privacy does not justify *Katz*'s elevation of privacy as the *sine qua non* of the Amendment. See T. Clancy, The Fourth Amendment: Its History and Interpretation §3.4.4, p. 78 (2008) ("[The *Katz* test] confuse[s] the reasons for exercising the protected right with the right itself. A purpose of exercising one's Fourth Amendment rights might be the desire for privacy, but the individual's motivation is not the right protected"); cf. *United States* v. *Gonzalez-Lopez*, 548 U. S. 140, 145 (2006) (rejecting "a line of reasoning that 'abstracts from the right to its purposes, and then eliminates the right'"). As the majority opinion in *Katz* recognized, the Fourth Amendment "cannot be translated into a general constitutional 'right to privacy,'" as its protections "often have nothing to do with privacy at all." 389 U. S., at 350. Justice Harlan's focus on privacy in his concurrence—an opinion that was issued between *Griswold* v. *Connecticut*, 381 U. S. 479 (1965), and *Roe* v. *Wade*, 410 U. S. 113 (1973)—reflects privacy's status as the organizing constitutional idea of the 1960's and 1970's. The organizing constitutional idea of the founding era, by contrast, was property.

C

In shifting the focus of the Fourth Amendment from property to privacy, the *Katz* test also reads the words

"persons, houses, papers, and effects" out of the text. At its broadest formulation, the *Katz* test would find a search "*wherever* an individual may harbor a reasonable 'expectation of privacy.'" *Terry*, 392 U. S., at 9 (emphasis added). The Court today, for example, does not ask whether cell-site location records are "persons, houses, papers, [or] effects" within the meaning of the Fourth Amendment.[8] Yet "persons, houses, papers, and effects" cannot mean "anywhere" or "anything." *Katz*'s catchphrase that "the Fourth Amendment protects people, not places," is not a serious attempt to reconcile the constitutional text. See *Carter*, 525 U. S., at 98, n. 3 (opinion of Scalia, J.). The Fourth Amendment obviously protects people; "[t]he question . . . is what protection it affords to those people." *Katz*, 389 U. S., at 361 (Harlan, J., concurring). The Founders decided to protect the people from unreasonable searches and seizures of four specific things—persons, houses, papers, and effects. They identified those four categories as "the objects of privacy protection to which the *Constitution* would extend, leaving further expansion to the good judgment . . . of the people through their representatives in the legislature." *Carter*, *supra*, at 97–98 (opinion of Scalia, J.).

This limiting language was important to the founders. Madison's first draft of the Fourth Amendment used a different phrase: "their persons, their houses, their papers, and their *other property*." 1 Annals of Cong. 452 (1789)

---

[8] The answer to that question is not obvious. Cell-site location records are business records that mechanically collect the interactions between a person's cell phone and the company's towers; they are not private papers and do not reveal the contents of any communications. Cf. Schnapper, Unreasonable Searches and Seizures of Papers, 71 Va. L. Rev. 869, 923–924 (1985) (explaining that business records that do not reveal "personal or speech-related confidences" might not satisfy the original meaning of "papers").

(emphasis added). In one of the few changes made to Madison's draft, the House Committee of Eleven changed "other property" to "effects." See House Committee of Eleven Report (July 28, 1789), in N. Cogan, The Complete Bill of Rights 334 (2d ed. 2015). This change might have narrowed the Fourth Amendment by clarifying that it does not protect real property (other than houses). See *Oliver* v. *United States*, 466 U. S. 170, 177, and n. 7 (1984); Davies, Recovering the Original Fourth Amendment, 98 Mich. L. Rev. 547, 709–714 (1999) (Davies). Or the change might have broadened the Fourth Amendment by clarifying that it protects commercial goods, not just personal possessions. See Donahue 1301. Or it might have done both. Whatever its ultimate effect, the change reveals that the Founders understood the phrase "persons, houses, papers, and effects" to be an important measure of the Fourth Amendment's overall scope. See Davies 710. The *Katz* test, however, displaces and renders that phrase entirely "superfluous." *Jones*, 565 U. S., at 405.

D

"[P]ersons, houses, papers, and effects" are not the only words that the *Katz* test reads out of the Fourth Amendment. The Fourth Amendment specifies that the people have a right to be secure from unreasonable searches of "their" persons, houses, papers, and effects. Although phrased in the plural, "[t]he obvious meaning of ['their'] is that *each* person has the right to be secure against unreasonable searches and seizures in *his own* person, house, papers, and effects." *Carter*, *supra*, at 92 (opinion of Scalia, J.); see also *District of Columbia* v. *Heller*, 554 U. S. 570, 579 (2008) (explaining that the Constitution uses the plural phrase "the people" to "refer to individual rights, not 'collective' rights"). Stated differently, the word "their" means, at the very least, that individuals do not have Fourth Amendment rights in *someone else's* property. See

Carter, *supra*, at 92–94 (opinion of Scalia, J.). Yet, under the *Katz* test, individuals can have a reasonable expectation of privacy in another person's property. See, *e.g., Carter*, 525 U. S., at 89 (majority opinion) ("[A] person may have a legitimate expectation of privacy in the house of someone else"). Until today, our precedents have not acknowledged that individuals can claim a reasonable expectation of privacy in someone else's business records. See *ante,* at 2 (KENNEDY, J., dissenting). But the Court erases that line in this case, at least for cell-site location records. In doing so, it confirms that the *Katz* test does not necessarily require an individual to prove that the government searched *his* person, house, paper, or effect.

Carpenter attempts to argue that the cell-site records are, in fact, his "papers," see Brief for Petitioner 32–35; Reply Brief 14–15, but his arguments are unpersuasive, see *ante,* at 12–13 (opinion of KENNEDY, J.); *post,* at 20–23 (ALITO, J., dissenting). Carpenter stipulated below that the cell-site records are the business records of Sprint and MetroPCS. See App. 51. He cites no property law in his briefs to this Court, and he does not explain how he has a property right in the companies' records under the law of any jurisdiction at any point in American history. If someone stole these records from Sprint or MetroPCS, Carpenter does not argue that he could recover in a traditional tort action. Nor do his contracts with Sprint and MetroPCS make the records his, even though such provisions could exist in the marketplace. Cf., *e.g.,* Google Terms of Service, https://policies.google.com/terms ("Some of our Services allow you to upload, submit, store, send or receive content. You retain ownership of any intellectual property rights that you hold in that content. In short, what belongs to you stays yours").

Instead of property, tort, or contract law, Carpenter relies on the federal Telecommunications Act of 1996 to demonstrate that the cell site records are his papers. The

Telecommunications Act generally bars cell-phone companies from disclosing customers' cell site location information to the public. See 47 U. S. C. §222(c). This is sufficient to make the records his, Carpenter argues, because the Fourth Amendment merely requires him to identify a source of "positive law" that "protects against access by the public without consent." Brief for Petitioner 32–33 (citing Baude & Stern, The Positive Law Model of the Fourth Amendment, 129 Harv. L. Rev. 1821, 1825–1826 (2016); emphasis deleted).

Carpenter is mistaken. To come within the text of the Fourth Amendment, Carpenter must prove that the cell-site records are *his*; positive law is potentially relevant only insofar as it answers that question. The text of the Fourth Amendment cannot plausibly be read to mean "any violation of positive law" any more than it can plausibly be read to mean "any violation of a reasonable expectation of privacy."

Thus, the Telecommunications Act is insufficient because it does not give Carpenter a property right in the cell-site records. Section 222, titled "Privacy of customer information," protects customers' privacy by preventing cell-phone companies from disclosing sensitive information about them. The statute creates a "duty to protect the confidentiality" of information relating to customers, §222(a), and creates "[p]rivacy requirements" that limit the disclosure of that information, §222(c)(1). Nothing in the text pre-empts state property law or gives customers a property interest in the companies' business records (assuming Congress even has that authority).[9] Although

---

[9] Carpenter relies on an order from the Federal Communications Commission (FCC), which weakly states that "'*[t]o the extent* [a customer's location information] is property, . . . it is better understood as belonging to the customer, not the carrier.'" Brief for Petitioner 34, and n. 23 (quoting 13 FCC Rcd. 8061, 8093 ¶43 (1998); emphasis added).

§222 "protects the interests of individuals against wrongful uses or disclosures of personal data, the rationale for these legal protections has not historically been grounded on a perception that people have property rights in personal data as such." Samuelson, Privacy as Intellectual Property? 52 Stan. L. Rev. 1125, 1130–1131 (2000) (footnote omitted). Any property rights remain with the companies.

E

The *Katz* test comes closer to the text of the Fourth Amendment when it asks whether an expectation of privacy is "reasonable," but it ultimately distorts that term as well. The Fourth Amendment forbids "unreasonable searches." In other words, reasonableness determines the legality of a search, not "whether a search . . . within the meaning of the Constitution has *occurred*." *Carter*, 525 U. S., at 97 (opinion of Scalia, J.) (internal quotation marks omitted).

Moreover, the *Katz* test invokes the concept of reasonableness in a way that would be foreign to the ratifiers of the Fourth Amendment. Originally, the word "unreasonable" in the Fourth Amendment likely meant "against reason"—as in "against the reason of the common law." See Donahue 1270–1275; Davies 686–693; *California* v. *Acevedo*, 500 U. S. 565, 583 (1991) (Scalia, J., concurring in judgment). At the founding, searches and seizures were

---

But this order was vacated by the Court of Appeals for the Tenth Circuit. *U. S. West, Inc.* v. *FCC*, 182 F. 3d 1224, 1240 (1999). Notably, the carrier in that case argued that the FCC's regulation of customer information was a taking of *its* property. See *id.,* at 1230. Although the panel majority had no occasion to address this argument, see *id.,* at 1239, n. 14, the dissent concluded that the carrier had failed to prove the information was "property" at all, see *id.,* at 1247–1248 (opinion of Briscoe, J.).

regulated by a robust body of common-law rules. See generally W. Cuddihy, The Fourth Amendment: Origins and Original Meaning 602–1791 (2009); *e.g., Wilson* v. *Arkansas*, 514 U. S. 927, 931–936 (1995) (discussing the common-law knock-and-announce rule). The search-and-seizure practices that the Founders feared most—such as general warrants—were already illegal under the common law, and jurists such as Lord Coke described violations of the common law as "against reason." See Donahue 1270–1271, and n. 513. Locke, Blackstone, Adams, and other influential figures shortened the phrase "against reason" to "unreasonable." See *id.,* at 1270–1275. Thus, by prohibiting "unreasonable" searches and seizures in the Fourth Amendment, the Founders ensured that the newly created Congress could not use legislation to abolish the established common-law rules of search and seizure. See T. Cooley, Constitutional Limitations *303 (2d ed. 1871); 3 J. Story, Commentaries on the Constitution of the United States §1895, p. 748 (1833).

Although the Court today maintains that its decision is based on "Founding-era understandings," *ante,* at 6, the Founders would be puzzled by the Court's conclusion as well as its reasoning. The Court holds that the Government unreasonably searched Carpenter by subpoenaing the cell-site records of Sprint and MetroPCS without a warrant. But the Founders would not recognize the Court's "warrant requirement." *Ante,* at 21. The common law required warrants for some types of searches and seizures, but not for many others. The relevant rule depended on context. See *Acevedo*, *supra*, at 583–584 (opinion of Scalia, J.); Amar, Fourth Amendment First Principles, 107 Harv. L. Rev. 757, 763–770 (1994); Davies 738–739. In cases like this one, a subpoena for third-party documents was not a "search" to begin with, and the common law did not limit the government's authority to subpoena third parties. See *post,* at 2–12 (ALITO, J., dissent-

ing). Suffice it to say, the Founders would be confused by this Court's transformation of their common-law protection of property into a "warrant requirement" and a vague inquiry into "reasonable expectations of privacy."

III

That the *Katz* test departs so far from the text of the Fourth Amendment is reason enough to reject it. But the *Katz* test also has proved unworkable in practice. Jurists and commentators tasked with deciphering our jurisprudence have described the *Katz* regime as "an unpredictable jumble," "a mass of contradictions and obscurities," "all over the map," "riddled with inconsistency and incoherence," "a series of inconsistent and bizarre results that [the Court] has left entirely undefended," "unstable," "chameleon-like," "'notoriously unhelpful,'" "a conclusion rather than a starting point for analysis," "distressingly unmanageable," "a dismal failure," "flawed to the core," "unadorned fiat," and "inspired by the kind of logic that produced Rube Goldberg's bizarre contraptions."[10] Even

---

[10] Kugler & Strahilevitz, Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory, 2015 S. Ct. Rev. 205, 261; Bradley, Two Models of the Fourth Amendment, 83 Mich. L. Rev. 1468 (1985); Kerr, Four Models of Fourth Amendment Protection, 60 Stan. L. Rev. 503, 505 (2007); Solove, Fourth Amendment Pragmatism, 51 Boston College L. Rev. 1511 (2010); Wasserstom & Seidman, The Fourth Amendment as Constitutional Theory, 77 Geo. L. J. 19, 29 (1988); Colb, What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy, 55 Stan. L. Rev. 119, 122 (2002); Clancy, The Fourth Amendment: Its History and Interpretation §3.3.4, p. 65 (2008); *Minnesota* v. *Carter*, 525 U. S. 83, 97 (1998) (Scalia, J., dissenting); *State* v. *Campbell*, 306 Ore. 157, 164, 759 P. 2d 1040, 1044 (1988); Wilkins, Defining the "Reasonable Expectation of Privacy": an Emerging Tripartite Analysis, 40 Vand. L. Rev. 1077, 1107 (1987); Yeager, Search, Seizure and the Positive Law: Expectations of Privacy Outside the Fourth Amendment, 84 J. Crim. L. & C. 249, 251 (1993); Thomas, Time Travel, Hovercrafts, and the Framers:

Justice Harlan, four years after penning his concurrence in *Katz*, confessed that the test encouraged "the substitution of words for analysis." *United States* v. *White*, 401 U. S. 745, 786 (1971) (dissenting opinion).

After 50 years, it is still unclear what question the *Katz* test is even asking. This Court has steadfastly declined to elaborate the relevant considerations or identify any meaningful constraints. See, *e.g., ante,* at 5 ("[N]o single rubric definitively resolves which expectations of privacy are entitled to protection"); *O'Connor* v. *Ortega*, 480 U. S. 709, 715 (1987) (plurality opinion) ("We have no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable"); *Oliver*, 466 U. S., at 177 ("No single factor determines whether an individual legitimately may claim under the Fourth Amendment that a place should be free of government intrusion").

Justice Harlan's original formulation of the *Katz* test appears to ask a descriptive question: Whether a given expectation of privacy is "one that society is prepared to recognize as 'reasonable.'" 389 U. S., at 361. As written, the *Katz* test turns on society's actual, current views about the reasonableness of various expectations of privacy.

But this descriptive understanding presents several problems. For starters, it is easily circumvented. If, for example, "the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry," individuals could not realistically expect privacy in their homes. *Smith*, 442 U. S., at 740, n. 5; see also Chemerinsky, Rediscovering Brandeis's

---

James Madison Sees the Future and Rewrites the Fourth Amendment, 80 Notre Dame L. Rev. 1451, 1500 (2005); *Rakas* v. *Illinois*, 439 U. S. 128, 165 (1978) (White, J., dissenting); Cloud, Rube Goldberg Meets the Constitution: The Supreme Court, Technology, and the Fourth Amendment, 72 Miss. L. J. 5, 7 (2002).

Right to Privacy, 45 Brandeis L. J. 643, 650 (2007) ("[Under *Katz,* t]he government seemingly can deny privacy just by letting people know in advance not to expect any"). A purely descriptive understanding of the *Katz* test also risks "circular[ity]." *Kyllo*, 533 U. S., at 34. While this Court is supposed to base its decisions on society's expectations of privacy, society's expectations of privacy are, in turn, shaped by this Court's decisions. See Posner, The Uncertain Protection of Privacy by the Supreme Court, 1979 S. Ct. Rev. 173, 188 ("[W]hether [a person] will or will not have [a reasonable] expectation [of privacy] will depend on what the legal rule is").

To address this circularity problem, the Court has insisted that expectations of privacy must come from outside its Fourth Amendment precedents, "either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." *Rakas* v. *Illinois*, 439 U. S. 128, 144, n. 12 (1978). But the Court's supposed reliance on "real or personal property law" rings hollow. The whole point of *Katz* was to "'discredi[t]'" the relationship between the Fourth Amendment and property law, 389 U. S., at 353, and this Court has repeatedly downplayed the importance of property law under the *Katz* test, see, *e.g., United States* v. *Salvucci*, 448 U. S. 83, 91 (1980) ("[P]roperty rights are neither the beginning nor the end of this Court's inquiry [under *Katz*]"); *Rawlings* v. *Kentucky*, 448 U. S. 98, 105 (1980) ("[This Court has] emphatically rejected the notion that 'arcane' concepts of property law ought to control the ability to claim the protections of the Fourth Amendment"). Today, for example, the Court makes no mention of property law, except to reject its relevance. See *ante,* at 5, and n. 1.

As for "understandings that are recognized or permitted in society," this Court has never answered even the most basic questions about what this means. See Kerr, Four

Models of Fourth Amendment Protection, 60 Stan. L. Rev. 503, 504–505 (2007). For example, our precedents do not explain who is included in "society," how we know what they "recogniz[e] or permi[t]," and how much of society must agree before something constitutes an "understanding."

Here, for example, society might prefer a balanced regime that prohibits the Government from obtaining cell-site location information unless it can persuade a neutral magistrate that the information bears on an ongoing criminal investigation. That is precisely the regime Congress created under the Stored Communications Act and Telecommunications Act. See 47 U. S. C. §222(c)(1); 18 U. S. C. §§2703(c)(1)(B), (d). With no sense of irony, the Court invalidates this regime today—the one that society actually created "in the form of its elected representatives in Congress." 819 F. 3d 880, 890 (2016).

Truth be told, this Court does not treat the *Katz* test as a descriptive inquiry. Although the *Katz* test is phrased in descriptive terms about society's views, this Court treats it like a normative question—whether a particular practice *should* be considered a search under the Fourth Amendment. Justice Harlan thought this was the best way to understand his test. See *White*, 401 U. S., at 786 (dissenting opinion) (explaining that courts must assess the "desirability" of privacy expectations and ask whether courts "should" recognize them by "balanc[ing]" the "impact on the individual's sense of security . . . against the utility of the conduct as a technique of law enforcement"). And a normative understanding is the only way to make sense of this Court's precedents, which bear the hallmarks of subjective policymaking instead of neutral legal decisionmaking. "[T]he only thing the past three decades have established about the *Katz* test" is that society's expectations of privacy "bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable."

Carter, 525 U. S., at 97 (opinion of Scalia, J.). Yet, "[t]hough we know ourselves to be eminently reasonable, self-awareness of eminent reasonableness is not really a substitute for democratic election." *Sosa* v. *Alvarez-Machain*, 542 U. S. 692, 750 (2004) (Scalia, J., concurring in part and concurring in judgment).

* * *

In several recent decisions, this Court has declined to apply the *Katz* test because it threatened to narrow the original scope of the Fourth Amendment. See *Grady* v. *North Carolina*, 575 U. S. ___, ___ (2015) (*per curiam*) (slip op., at 3); *Florida* v. *Jardines*, 569 U. S. 1, 5 (2013); *Jones*, 565 U. S., at 406–407. But as today's decision demonstrates, *Katz* can also be invoked to expand the Fourth Amendment beyond its original scope. This Court should not tolerate errors in either direction. "The People, through ratification, have already weighed the policy tradeoffs that constitutional rights entail." *Luis* v. *United States*, 578 U. S. ___, ___ (2016) (THOMAS, J., concurring in judgment) (slip op., at 10). Whether the rights they ratified are too broad or too narrow by modern lights, this Court has no authority to unilaterally alter the document they approved.

Because the *Katz* test is a failed experiment, this Court is dutybound to reconsider it. Until it does, I agree with my dissenting colleagues' reading of our precedents. Accordingly, I respectfully dissent.

SUPREME COURT OF THE UNITED STATES

No. 16–402

TIMOTHY IVORY CARPENTER, PETITIONER *v.* UNITED STATES

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

[June 22, 2018]

JUSTICE ALITO, with whom JUSTICE THOMAS joins, dissenting.

I share the Court's concern about the effect of new technology on personal privacy, but I fear that today's decision will do far more harm than good. The Court's reasoning fractures two fundamental pillars of Fourth Amendment law, and in doing so, it guarantees a blizzard of litigation while threatening many legitimate and valuable investigative practices upon which law enforcement has rightfully come to rely.

First, 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. It violates both the original understanding of the Fourth Amendment and more than a century of Supreme Court precedent. Unless it is somehow restricted to the particular situation in the present case, the Court's move will cause upheaval. Must every grand jury subpoena *duces tecum* be supported by probable cause? If so, investigations of terrorism, political

corruption, white-collar crime, and many other offenses will be stymied. And what about subpoenas and other document-production orders issued by administrative agencies? See, *e.g.*, 15 U. S. C. §57b–1(c) (Federal Trade Commission); §§77s(c), 78u(a)–(b) (Securities and Exchange Commission); 29 U. S. C. §657(b) (Occupational Safety and Health Administration); 29 CFR §1601.16(a)(2) (2017) (Equal Employment Opportunity Commission).

Second, the Court allows a defendant to object to the search of a third party's property. This also is revolutionary. The Fourth Amendment protects "[t]he right of the people to be secure in *their* persons, houses, papers, and effects" (emphasis added), not the persons, houses, papers, and effects of others. Until today, we have been careful to heed this fundamental feature of the Amendment's text. This was true when the Fourth Amendment was tied to property law, and it remained true after *Katz* v. *United States*, 389 U. S. 347 (1967), broadened the Amendment's reach.

By departing dramatically from these fundamental principles, the Court destabilizes long-established Fourth Amendment doctrine. We will be making repairs—or picking up the pieces—for a long time to come.

I

Today the majority holds that a court order requiring the production of cell-site records may be issued only after the Government demonstrates probable cause. See *ante*, at 18. That is a serious and consequential mistake. The Court's holding is based on the premise that the order issued in this case was an actual "search" within the meaning of the Fourth Amendment, but that premise is inconsistent with the original meaning of the Fourth Amendment and with more than a century of precedent.

A

The order in this case was the functional equivalent of a subpoena for documents, and there is no evidence that these writs were regarded as "searches" at the time of the founding. Subpoenas *duces tecum* and other forms of compulsory document production were well known to the founding generation. Blackstone dated the first writ of subpoena to the reign of King Richard II in the late 14th century, and by the end of the 15th century, the use of such writs had "become the daily practice of the [Chancery] court." 3 W. Blackstone, Commentaries on the Laws of England 53 (G. Tucker ed. 1803) (Blackstone). Over the next 200 years, subpoenas would grow in prominence and power in tandem with the Court of Chancery, and by the end of Charles II's reign in 1685, two important innovations had occurred.

First, the Court of Chancery developed a new species of subpoena. Until this point, subpoenas had been used largely to compel attendance and oral testimony from witnesses; these subpoenas correspond to today's subpoenas *ad testificandum*. But the Court of Chancery also improvised a new version of the writ that tacked onto a regular subpoena an order compelling the witness to bring certain items with him. By issuing these so-called subpoenas *duces tecum*, the Court of Chancery could compel the production of papers, books, and other forms of physical evidence, whether from the parties to the case or from third parties. Such subpoenas were sufficiently commonplace by 1623 that a leading treatise on the practice of law could refer in passing to the fee for a "*Sub pœna* of *Ducas tecum*" (seven shillings and two pence) without needing to elaborate further. T. Powell, The Attourneys Academy 79 (1623). Subpoenas *duces tecum* would swell in use over the next century as the rules for their application became ever more developed and definite. See, *e.g.*, 1 G. Jacob, The Compleat Chancery-Practiser 290 (1730) ("The *Sub-*

poena duces tecum is awarded when the Defendant has confessed by his Answer that he hath such Writings in his Hands as are prayed by the Bill to be discovered or brought into Court").

Second, although this new species of subpoena had its origins in the Court of Chancery, it soon made an appearance in the work of the common-law courts as well. One court later reported that "[t]he Courts of Common law . . . employed the same or similar means . . . from the time of Charles the Second at least." *Amey* v. *Long*, 9 East. 473, 484, 103 Eng. Rep. 653, 658 (K. B. 1808).

By the time Blackstone published his Commentaries on the Laws of England in the 1760's, the use of subpoenas *duces tecum* had bled over substantially from the courts of equity to the common-law courts. Admittedly, the transition was still incomplete: In the context of jury trials, for example, Blackstone complained about "the want of a compulsive power for the production of books and papers belonging to the parties." Blackstone 381; see also, *e.g.*, *Entick* v. *Carrington*, 19 State Trials 1029, 1073 (K. B. 1765) ("I wish some cases had been shewn, where the law forceth evidence out of the owner's custody by process. [But] where the adversary has by force or fraud got possession of your own proper evidence, there is no way to get it back but by action"). But Blackstone found some comfort in the fact that at least those documents "[i]n the hands of third persons . . . can generally be obtained by rule of court, or by adding a clause of requisition to the writ of *subpoena*, which is then called a *subpoena duces tecum*." Blackstone 381; see also, *e.g.*, *Leeds* v. *Cook*, 4 Esp. 256, 257, 170 Eng. Rep. 711 (N. P. 1803) (third-party subpoena *duces tecum*); *Rex* v. *Babb*, 3 T. R. 579, 580, 100 Eng. Rep. 743, 744 (K. B. 1790) (third-party document production). One of the primary questions outstanding, then, was whether common-law courts would remedy the "defect[s]" identified by the Commentaries, and allow

parties to use subpoenas *duces tecum* not only with respect to third parties but also with respect to each other. Blackstone 381.

That question soon found an affirmative answer on both sides of the Atlantic. In the United States, the First Congress established the federal court system in the Judiciary Act of 1789. As part of that Act, Congress authorized "all the said courts of the United States . . . in the trial of actions at law, on motion and due notice thereof being given, to require the parties to produce books or writings in their possession or power, which contain evidence pertinent to the issue, in cases and under circumstances where they might be compelled to produce the same by the ordinary rules of proceeding in chancery." §15, 1 Stat. 82. From that point forward, federal courts in the United States could compel the production of documents regardless of whether those documents were held by parties to the case or by third parties.

In Great Britain, too, it was soon definitively established that common-law courts, like their counterparts in equity, could subpoena documents held either by parties to the case or by third parties. After proceeding in fits and starts, the King's Bench eventually held in *Amey* v. *Long* that the "writ of subpœna duces tecum [is] a writ of compulsory obligation and effect in the law." 9 East., at 486, 103 Eng. Rep., at 658. Writing for a unanimous court, Lord Chief Justice Ellenborough explained that "[t]he right to resort to means competent to compel the production of written, as well as oral, testimony seems essential to the very existence and constitution of a Court of Common Law." *Id.,* at 484, 103 Eng. Rep., at 658. Without the power to issue subpoenas *duces tecum*, the Lord Chief Justice observed, common-law courts "could not possibly proceed with due effect." *Ibid.*

The prevalence of subpoenas *duces tecum* at the time of the founding was not limited to the civil context. In crim-

inal cases, courts and prosecutors were also using the writ to compel the production of necessary documents. In *Rex* v. *Dixon*, 3 Burr. 1687, 97 Eng. Rep. 1047 (K. B. 1765), for example, the King's Bench considered the propriety of a subpoena *duces tecum* served on an attorney named Samuel Dixon. Dixon had been called "to give evidence before the grand jury of the county of Northampton" and specifically "to produce three vouchers . . . in order to found a prosecution by way of indictment against [his client] Peach . . . for forgery." *Id.,* at 1687, 97 Eng. Rep., at 1047–1048. Although the court ultimately held that Dixon had not needed to produce the vouchers on account of attorney-client privilege, none of the justices expressed the slightest doubt about the general propriety of subpoenas *duces tecum* in the criminal context. See *id.,* at 1688, 97 Eng. Rep., at 1048. As Lord Chief Justice Ellenborough later explained, "[i]n that case no objection was taken to the writ, but to the special circumstances under which the party possessed the papers; so that the Court may be considered as recognizing the general obligation to obey writs of that description in other cases." *Amey*, *supra*, at 485, 103 Eng. Rep., at 658; see also 4 J. Chitty, Practical Treatise on the Criminal Law 185 (1816) (template for criminal subpoena *duces tecum*).

As *Dixon* shows, subpoenas *duces tecum* were routine in part because of their close association with grand juries. Early American colonists imported the grand jury, like so many other common-law traditions, and they quickly flourished. See *United States* v. *Calandra*, 414 U. S. 338, 342–343 (1974). Grand juries were empaneled by the federal courts almost as soon as the latter were established, and both they and their state counterparts actively exercised their wide-ranging common-law authority. See R. Younger, The People's Panel 47–55 (1963). Indeed, "the Founders thought the grand jury so essential . . . that they provided in the Fifth Amendment that federal prosecution

for serious crimes can only be instituted by 'a presentment or indictment of a Grand Jury.'" *Calandra*, *supra*, at 343.

Given the popularity and prevalence of grand juries at the time, the Founders must have been intimately familiar with the tools they used—including compulsory process—to accomplish their work. As a matter of tradition, grand juries were "accorded wide latitude to inquire into violations of criminal law," including the power to "compel the production of evidence or the testimony of witnesses as [they] conside[r] appropriate." *Ibid.* Long before national independence was achieved, grand juries were already using their broad inquisitorial powers not only to present and indict criminal suspects but also to inspect public buildings, to levy taxes, to supervise the administration of the laws, to advance municipal reforms such as street repair and bridge maintenance, and in some cases even to propose legislation. Younger, *supra*, at 5–26. Of course, such work depended entirely on grand juries' ability to access any relevant documents.

Grand juries continued to exercise these broad inquisitorial powers up through the time of the founding. See *Blair* v. *United States*, 250 U. S. 273, 280 (1919) ("At the foundation of our Federal Government the inquisitorial function of the grand jury and the compulsion of witnesses were recognized as incidents of the judicial power"). In a series of lectures delivered in the early 1790's, Justice James Wilson crowed that grand juries were "the peculiar boast of the common law" thanks in part to their wide-ranging authority: "All the operations of government, and of its ministers and officers, are within the compass of their view and research." 2 J. Wilson, The Works of James Wilson 534, 537 (R. McCloskey ed. 1967). That reflected the broader insight that "[t]he grand jury's investigative power must be broad if its public responsibility is adequately to be discharged." *Calandra*, *supra*, at 344.

Compulsory process was also familiar to the founding

generation in part because it reflected "the ancient proposition of law" that "'"the public . . . has a right to every man's evidence."'" *United States* v. *Nixon*, 418 U. S. 683, 709 (1974); see also *ante*, at 10 (KENNEDY, J., dissenting). As early as 1612, "Lord Bacon is reported to have declared that 'all subjects, without distinction of degrees, owe to the King tribute and service, not only of their deed and hand, but of their knowledge and discovery.'" *Blair*, *supra*, at 279–280. That duty could be "onerous at times," yet the Founders considered it "necessary to the administration of justice according to the forms and modes established in our system of government." *Id.,* at 281; see also *Calandra*, *supra*, at 345.

B

Talk of kings and common-law writs may seem out of place in a case about cell-site records and the protections afforded by the Fourth Amendment in the modern age. But this history matters, not least because it tells us what was on the minds of those who ratified the Fourth Amendment and how they understood its scope. That history makes it abundantly clear that the Fourth Amendment, as originally understood, did not apply to the compulsory production of documents at all.

The Fourth Amendment does not regulate all methods by which the Government obtains documents. Rather, it prohibits only those "searches and seizures" of "persons, houses, papers, and effects" that are "unreasonable." Consistent with that language, "at least until the latter half of the 20th century" "our Fourth Amendment jurisprudence was tied to common-law trespass." *United States* v. *Jones*, 565 U. S. 400, 405 (2012). So by its terms, the Fourth Amendment does not apply to the compulsory production of documents, a practice that involves neither any physical intrusion into private space nor any taking of property by agents of the state. Even Justice Brandeis—a

stalwart proponent of construing the Fourth Amendment liberally—acknowledged that "under any ordinary construction of language," "there is no 'search' or 'seizure' when a defendant is required to produce a document in the orderly process of a court's procedure." *Olmstead* v. *United States*, 277 U. S. 438, 476 (1928) (dissenting opinion).[1]

Nor is there any reason to believe that the Founders intended the Fourth Amendment to regulate courts' use of compulsory process. American colonists rebelled against the Crown's physical invasions of their persons and their property, not against its acquisition of information by any and all means. As Justice Black once put it, "[t]he Fourth Amendment was aimed directly at the abhorred practice of breaking in, ransacking and searching homes and other buildings and seizing people's personal belongings without warrants issued by magistrates." *Katz*, 389 U. S., at 367 (dissenting opinion). More recently, we have acknowledged that "the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed

---

[1]Any other interpretation of the Fourth Amendment's text would run into insuperable problems because it would apply not only to subpoenas *duces tecum* but to all other forms of compulsory process as well. If the Fourth Amendment applies to the compelled production of documents, then it must also apply to the compelled production of testimony—an outcome that we have repeatedly rejected and which, if accepted, would send much of the field of criminal procedure into a tailspin. See, *e.g.*, *United States* v. *Dionisio*, 410 U. S. 1, 9 (1973) ("It is clear that a subpoena to appear before a grand jury is not a 'seizure' in the Fourth Amendment sense, even though that summons may be inconvenient or burdensome"); *United States* v. *Calandra*, 414 U. S. 338, 354 (1974) ("Grand jury questions . . . involve no independent governmental invasion of one's person, house, papers, or effects"). As a matter of original understanding, a subpoena *duces tecum* no more effects a "search" or "seizure" of papers within the meaning of the Fourth Amendment than a subpoena *ad testificandum* effects a "search" or "seizure" of a person.

British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley* v. *California*, 573 U. S. ___, ___ (2014) (slip op., at 27).

General warrants and writs of assistance were noxious not because they allowed the Government to acquire evidence in criminal investigations, but because of the *means* by which they permitted the Government to acquire that evidence. Then, as today, searches could be quite invasive. Searches generally begin with officers "mak[ing] nonconsensual entries into areas not open to the public." *Donovan* v. *Lone Steer, Inc.*, 464 U. S. 408, 414 (1984). Once there, officers are necessarily in a position to observe private spaces generally shielded from the public and discernible only with the owner's consent. Private area after private area becomes exposed to the officers' eyes as they rummage through the owner's property in their hunt for the object or objects of the search. If they are searching for documents, officers may additionally have to rifle through many other papers—potentially filled with the most intimate details of a person's thoughts and life—before they find the specific information they are seeking. See *Andresen* v. *Maryland*, 427 U. S. 463, 482, n. 11 (1976). If anything sufficiently incriminating comes into view, officers seize it. *Horton* v. *California*, 496 U. S. 128, 136–137 (1990). Physical destruction always lurks as an underlying possibility; "officers executing search warrants on occasion must damage property in order to perform their duty." *Dalia* v. *United States*, 441 U. S. 238, 258 (1979); see, *e.g.*, *United States* v. *Ramirez*, 523 U. S. 65, 71–72 (1998) (breaking garage window); *United States* v. *Ross*, 456 U. S. 798, 817–818 (1982) (ripping open car upholstery); *Brown* v. *Battle Creek Police Dept.*, 844 F. 3d 556, 572 (CA6 2016) (shooting and killing two pet dogs); *Lawmaster* v. *Ward*, 125 F. 3d 1341, 1350, n. 3 (CA10 1997) (breaking locks).

Compliance with a subpoena *duces tecum* requires none

of that. A subpoena *duces tecum* permits a subpoenaed individual to conduct the search for the relevant documents himself, without law enforcement officers entering his home or rooting through his papers and effects. As a result, subpoenas avoid the many incidental invasions of privacy that necessarily accompany any actual search. And it was *those* invasions of privacy—which, although incidental, could often be extremely intrusive and damaging—that led to the adoption of the Fourth Amendment.

Neither this Court nor any of the parties have offered the slightest bit of historical evidence to support the idea that the Fourth Amendment originally applied to subpoenas *duces tecum* and other forms of compulsory process. That is telling, for as I have explained, these forms of compulsory process were a feature of criminal (and civil) procedure well known to the Founders. The Founders would thus have understood that holding the compulsory production of documents to the same standard as actual searches and seizures would cripple the work of courts in civil and criminal cases alike. It would be remarkable to think that, despite that knowledge, the Founders would have gone ahead and sought to impose such a requirement. It would be even more incredible to believe that the Founders would have imposed that requirement through the inapt vehicle of an amendment directed at different concerns. But it would blink reality entirely to argue that this entire process happened without anyone saying *the least thing about it*—not during the drafting of the Bill of Rights, not during any of the subsequent ratification debates, and not for most of the century that followed. If the Founders thought the Fourth Amendment applied to the compulsory production of documents, one would imagine that there would be *some* founding-era evidence of the Fourth Amendment being applied to the compulsory production of documents. Cf. *Free Enterprise Fund* v. *Public Company Accounting Oversight Bd.*, 561 U. S. 477, 505

(2010); *Printz* v. *United States*, 521 U. S. 898, 905 (1997). Yet none has been brought to our attention.

C

Of course, our jurisprudence has not stood still since 1791. We now evaluate subpoenas *duces tecum* and other forms of compulsory document production under the Fourth Amendment, although we employ a reasonableness standard that is less demanding than the requirements for a warrant. But the road to that doctrinal destination was anything but smooth, and our initial missteps—and the subsequent struggle to extricate ourselves from their consequences—should provide an object lesson for today's majority about the dangers of holding compulsory process to the same standard as actual searches and seizures.

For almost a century after the Fourth Amendment was enacted, this Court said and did nothing to indicate that it might regulate the compulsory production of documents. But that changed temporarily when the Court decided *Boyd* v. *United States*, 116 U. S. 616 (1886), the first—and, until today, the only—case in which this Court has ever held the compulsory production of documents to the same standard as actual searches and seizures.

The *Boyd* Court held that a court order compelling a company to produce potentially incriminating business records violated both the Fourth and the Fifth Amendments. The Court acknowledged that "certain aggravating incidents of actual search and seizure, such as forcible entry into a man's house and searching amongst his papers, are wanting" when the Government relies on compulsory process. *Id.*, at 622. But it nevertheless asserted that the Fourth Amendment ought to "be liberally construed," *id.*, at 635, and further reasoned that compulsory process "effects the sole object and purpose of search and seizure" by "forcing from a party evidence against himself," *id.*, at 622. "In this regard," the Court concluded,

"the Fourth and Fifth Amendments run almost into each other." *Id.*, at 630. Having equated compulsory process with actual searches and seizures and having melded the Fourth Amendment with the Fifth, the Court then found the order at issue unconstitutional because it compelled the production of property to which the Government did not have superior title. See *id.*, at 622–630.

In a concurrence joined by Chief Justice Waite, Justice Miller agreed that the order violated the Fifth Amendment, *id.*, at 639, but he strongly protested the majority's invocation of the Fourth Amendment. He explained: "[T]here is no reason why this court should assume that the action of the court below, in requiring a party to produce certain papers . . . , authorizes an unreasonable search or seizure of the house, papers, or effects of that party. There is in fact no search and no seizure." *Ibid.* "If the mere service of a notice to produce a paper . . . is a search," Justice Miller concluded, "then a change has taken place in the meaning of words, which has not come within my reading, and which I think was unknown at the time the Constitution was made." *Id.,* at 641.

Although *Boyd* was replete with stirring rhetoric, its reasoning was confused from start to finish in a way that ultimately made the decision unworkable. See 3 W. LaFave, J. Israel, N. King, & O. Kerr, Criminal Procedure §8.7(a) (4th ed. 2015). Over the next 50 years, the Court would gradually roll back *Boyd*'s erroneous conflation of compulsory process with actual searches and seizures.

That effort took its first significant stride in *Hale* v. *Henkel*, 201 U. S. 43 (1906), where the Court found it "quite clear" and "conclusive" that "the search and seizure clause of the Fourth Amendment was not intended to interfere with the power of courts to compel, through a *subpœna duces tecum*, the production, upon a trial in court, of documentary evidence." *Id.,* at 73. Without that writ, the Court recognized, "it would be 'utterly impossible

to carry on the administration of justice.'" *Ibid.*

Hale, however, did not entirely liberate subpoenas *duces tecum* from Fourth Amendment constraints. While refusing to treat such subpoenas as the equivalent of actual searches, *Hale* concluded that they must not be unreasonable. And it held that the subpoena *duces tecum* at issue was "far too sweeping in its terms to be regarded as reasonable." *Id.,* at 76. The *Hale* Court thus left two critical questions unanswered: Under the Fourth Amendment, what makes the compulsory production of documents "reasonable," and how does that standard differ from the one that governs actual searches and seizures?

The Court answered both of those questions definitively in *Oklahoma Press Publishing Co.* v. *Walling*, 327 U. S. 186 (1946), where we held that the Fourth Amendment regulates the compelled production of documents, but less stringently than it does full-blown searches and seizures. *Oklahoma Press* began by admitting that the Court's opinions on the subject had "perhaps too often . . . been generative of heat rather than light," "mov[ing] with variant direction" and sometimes having "highly contrasting" "emphasis and tone." *Id.,* at 202. "The primary source of misconception concerning the Fourth Amendment's function" in this context, the Court explained, "lies perhaps in the identification of cases involving so-called 'figurative' or 'constructive' search with cases of actual search and seizure." *Ibid.* But the Court held that "the basic distinction" between the compulsory production of documents on the one hand, and actual searches and seizures on the other, meant that two different standards had to be applied. *Id.,* at 204.

Having reversed *Boyd*'s conflation of the compelled production of documents with actual searches and seizures, the Court then set forth the relevant Fourth Amendment standard for the former. When it comes to "the production of corporate or other business records," the

Court held that the Fourth Amendment "at the most guards against abuse only by way of too much indefiniteness or breadth in the things required to be 'particularly described,' if also the inquiry is one the demanding agency is authorized by law to make and the materials specified are relevant." *Oklahoma Press*, *supra*, at 208. Notably, the Court held that a showing of probable cause was not necessary so long as "the investigation is authorized by Congress, is for a purpose Congress can order, and the documents sought are relevant to the inquiry." *Id.,* at 209.

Since *Oklahoma Press*, we have consistently hewed to that standard. See, *e.g.*, *Lone Steer, Inc.*, 464 U. S., at 414–415; *United States* v. *Miller*, 425 U. S. 435, 445–446 (1976); *California Bankers Assn.* v. *Shultz*, 416 U. S. 21, 67 (1974); *United States* v. *Dionisio*, 410 U. S. 1, 11–12 (1973); *See* v. *Seattle*, 387 U. S. 541, 544 (1967); *United States* v. *Powell*, 379 U. S. 48, 57–58 (1964); *McPhaul* v. *United States*, 364 U. S. 372, 382–383 (1960); *United States* v. *Morton Salt Co.*, 338 U. S. 632, 652–653 (1950); cf. *McLane Co.* v. *EEOC*, 581 U. S. ___, ___ (2017) (slip op., at 11). By applying *Oklahoma Press* and thereby respecting "the traditional distinction between a search warrant and a subpoena," *Miller*, *supra*, at 446, this Court has reinforced "the basic compromise" between "the public interest" in every man's evidence and the private interest "of men to be free from officious meddling." *Oklahoma Press*, *supra*, at 213.

D

Today, however, the majority inexplicably ignores the settled rule of *Oklahoma Press* in favor of a resurrected version of *Boyd*. That is mystifying. This should have been an easy case regardless of whether the Court looked to the original understanding of the Fourth Amendment or to our modern doctrine.

As a matter of original understanding, the Fourth

Amendment does not regulate the compelled production of documents at all. Here the Government received the relevant cell-site records pursuant to a court order compelling Carpenter's cell service provider to turn them over. That process is thus immune from challenge under the original understanding of the Fourth Amendment.

As a matter of modern doctrine, this case is equally straightforward. As JUSTICE KENNEDY explains, no search or seizure of Carpenter or his property occurred in this case. *Ante*, at 6–22; see also Part II, *infra*. But even if the majority were right that the Government "searched" Carpenter, it would at most be a "figurative or constructive search" governed by the *Oklahoma Press* standard, not an "actual search" controlled by the Fourth Amendment's warrant requirement.

And there is no doubt that the Government met the *Oklahoma Press* standard here. Under *Oklahoma Press*, a court order must "'be sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome.'" *Lone Steer, Inc.*, *supra*, at 415. Here, the type of order obtained by the Government almost necessarily satisfies that standard. The Stored Communications Act allows a court to issue the relevant type of order "only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that . . . the records . . . sough[t] are relevant and material to an ongoing criminal investigation." 18 U. S. C. §2703(d). And the court "may quash or modify such order" if the provider objects that the "records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider." *Ibid.* No such objection was made in this case, and Carpenter does not suggest that the orders contravened the *Oklahoma Press* standard in any other way.

That is what makes the majority's opinion so puzzling.

It decides that a "search" of Carpenter occurred within the meaning of the Fourth Amendment, but then it leaps straight to imposing requirements that—until this point—have governed only *actual* searches and seizures. See *ante*, at 18–19. Lost in its race to the finish is any real recognition of the century's worth of precedent it jeopardizes. For the majority, this case is apparently no different from one in which Government agents raided Carpenter's home and removed records associated with his cell phone.

Against centuries of precedent and practice, all that the Court can muster is the observation that "this Court has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy." *Ante*, at 19. Frankly, I cannot imagine a concession more damning to the Court's argument than that. As the Court well knows, the reason that we have never seen such a case is because—until today—defendants categorically had no "reasonable expectation of privacy" and no property interest in records belonging to third parties. See Part II, *infra*. By implying otherwise, the Court tries the nice trick of seeking shelter under the cover of precedents that it simultaneously perforates.

Not only that, but even if the Fourth Amendment permitted someone to object to the subpoena of a third party's records, the Court cannot explain why that individual should be entitled to *greater* Fourth Amendment protection than the party actually being subpoenaed. When parties are subpoenaed to turn over their records, after all, they will at most receive the protection afforded by *Oklahoma Press* even though they will own and have a reasonable expectation of privacy in the records at issue. Under the Court's decision, however, the Fourth Amendment will extend greater protections to someone else who is not being subpoenaed and does not own the records. That outcome makes no sense, and the Court does not even attempt to defend it.

We have set forth the relevant Fourth Amendment standard for subpoenaing business records many times over. Out of those dozens of cases, the majority cannot find even one that so much as suggests an exception to the *Oklahoma Press* standard for sufficiently personal information. Instead, we have always "described the constitutional requirements" for compulsory process as being "'settled'" and as applying categorically to all "'subpoenas [of] corporate books or records.'" *Lone Steer, Inc.*, 464 U. S., at 415 (internal quotation marks omitted). That standard, we have held, is "*the most*" protection the Fourth Amendment gives "to the production of corporate records and papers." *Oklahoma Press*, 327 U. S., at 208 (emphasis added).[2]

Although the majority announces its holding in the context of the Stored Communications Act, nothing stops its logic from sweeping much further. The Court has offered no meaningful limiting principle, and none is apparent. Cf. Tr. of Oral Arg. 31 (Carpenter's counsel admitting that "a grand jury subpoena . . . would be held to the same standard as any other subpoena or subpoena-like request for [cell-site] records").

Holding that subpoenas must meet the same standard as conventional searches will seriously damage, if not destroy, their utility. Even more so than at the founding, today the Government regularly uses subpoenas *duces tecum* and other forms of compulsory process to carry out its essential functions. See, *e.g.*, *Dionisio*, 410 U. S., at 11–12 (grand jury subpoenas); *McPhaul*, 364 U. S., at 382–383 (legislative subpoenas); *Oklahoma Press*, *supra*, at 208–209 (administrative subpoenas). Grand juries, for

---

[2] All that the Court can say in response is that we have "been careful not to uncritically extend existing precedents" when confronting new technologies. *Ante*, at 20. But applying a categorical rule categorically does not "extend" precedent, so the Court's statement ends up sounding a lot like a tacit admission that it is overruling our precedents.

example, have long "compel[led] the production of evidence" in order to determine "*whether* there is probable cause to believe a crime has been committed." *Calandra*, 414 U. S., at 343 (emphasis added). Almost by definition, then, grand juries will be unable at first to demonstrate "the probable cause required for a warrant." *Ante*, at 19 (majority opinion); see also *Oklahoma Press*, *supra*, at 213. If they are required to do so, the effects are as predictable as they are alarming: Many investigations will sputter out at the start, and a host of criminals will be able to evade law enforcement's reach.

"To ensure that justice is done, it is imperative to the function of courts that compulsory process be available for the production of evidence." *Nixon*, 418 U. S., at 709. For over a hundred years, we have understood that holding subpoenas to the same standard as actual searches and seizures "would stop much if not all of investigation in the public interest at the threshold of inquiry." *Oklahoma Press*, *supra*, at 213. Today a skeptical majority decides to put that understanding to the test.

II

Compounding its initial error, the Court also holds that a defendant has the right under the Fourth Amendment to object to the search of a third party's property. This holding flouts the clear text of the Fourth Amendment, and it cannot be defended under either a property-based interpretation of that Amendment or our decisions applying the reasonable-expectations-of-privacy test adopted in *Katz*, 389 U. S. 347. By allowing Carpenter to object to the search of a third party's property, the Court threatens to revolutionize a second and independent line of Fourth Amendment doctrine.

A

It bears repeating that the Fourth Amendment guaran-

tees "[t]he right of the people to be secure in *their* persons, houses, papers, and effects." (Emphasis added.) The Fourth Amendment does not confer rights with respect to the persons, houses, papers, and effects of others. Its language makes clear that "Fourth Amendment rights are personal," *Rakas* v. *Illinois*, 439 U. S. 128, 140 (1978), and as a result, this Court has long insisted that they "may not be asserted vicariously," *id.*, at 133. It follows that a "person who is aggrieved . . . only through the introduction of damaging evidence secured by a search of a third person's premises or property has not had any of his Fourth Amendment rights infringed." *Id.*, at 134.

In this case, as JUSTICE KENNEDY cogently explains, the cell-site records obtained by the Government belong to Carpenter's cell service providers, not to Carpenter. See *ante*, at 12–13. Carpenter did not create the cell-site records. Nor did he have possession of them; at all relevant times, they were kept by the providers. Once Carpenter subscribed to his provider's service, he had no right to prevent the company from creating or keeping the information in its records. Carpenter also had no right to demand that the providers destroy the records, no right to prevent the providers from destroying the records, and, indeed, no right to modify the records in any way whatsoever (or to prevent the providers from modifying the records). Carpenter, in short, has no meaningful control over the cell-site records, which are created, maintained, altered, used, and eventually destroyed by his cell service providers.

Carpenter responds by pointing to a provision of the Telecommunications Act that requires a provider to disclose cell-site records when a customer so requests. See 47 U. S. C. §222(c)(2). But a statutory disclosure requirement is hardly sufficient to give someone an ownership interest in the documents that must be copied and disclosed. Many statutes confer a right to obtain copies of documents

without creating any property right.[3]

Carpenter's argument is particularly hard to swallow because nothing in the Telecommunications Act precludes cell service providers from charging customers a fee for accessing cell-site records. See *ante*, at 12–13 (KENNEDY, J., dissenting). It would be very strange if the owner of records were required to pay in order to inspect his own

---

[3] See, *e.g.*, Freedom of Information Act, 5 U. S. C. §552(a) ("Each agency shall make available to the public information as follows . . ."); Privacy Act, 5 U. S. C. §552a(d)(1) ("Each agency that maintains a system of records shall . . . upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof . . ."); Fair Credit Reporting Act, 15 U. S. C. §1681j(a)(1)(A) ("All consumer reporting agencies . . . shall make all disclosures pursuant to section 1681g of this title once during any 12-month period upon request of the consumer and without charge to the consumer"); Right to Financial Privacy Act of 1978, 12 U. S. C. §3404(c) ("The customer has the right . . . to obtain a copy of the record which the financial institution shall keep of all instances in which the customer's record is disclosed to a Government authority pursuant to this section, including the identity of the Government authority to which such disclosure is made"); Government in the Sunshine Act, 5 U. S. C. §552b(f)(2) ("Copies of such transcript, or minutes, or a transcription of such recording disclosing the identity of each speaker, shall be furnished to any person at the actual cost of duplication or transcription"); Cable Act, 47 U. S. C. §551(d) ("A cable subscriber shall be provided access to all personally identifiable information regarding that subscriber which is collected and maintained by a cable operator"); Family Educational Rights and Privacy Act of 1974, 20 U. S. C. §1232g(a)(1)(A) ("No funds shall be made available under any applicable program to any educational agency or institution which has a policy of denying, or which effectively prevents, the parents of students who are or have been in attendance at a school of such agency or at such institution, as the case may be, the right to inspect and review the education records of their children. . . . Each educational agency or institution shall establish appropriate procedures for the granting of a request by parents for access to the education records of their children within a reasonable period of time, but in no case more than forty-five days after the request has been made").

property.

Nor does the Telecommunications Act give Carpenter a property right in the cell-site records simply because they are subject to confidentiality restrictions. See 47 U. S. C. §222(c)(1) (without a customer's permission, a cell service provider may generally "use, disclose, or permit access to individually identifiable [cell-site records]" only with respect to "its provision" of telecommunications services). Many federal statutes impose similar restrictions on private entities' use or dissemination of information in their own records without conferring a property right on third parties.[4]

---

[4] See, *e.g.*, Family Educational Rights and Privacy Act, 20 U. S. C. §1232g(b)(1) ("No funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of permitting the release of education records (or personally identifiable information contained therein other than directory information . . .) of students without the written consent of their parents to any individual, agency, or organization . . ."); Video Privacy Protection Act, 18 U. S. C. §2710(b)(1) ("A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (d)"); Driver Privacy Protection Act, 18 U. S. C. §2721(a)(1) ("A State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity . . . personal information . . ."); Fair Credit Reporting Act, 15 U. S. C. §1681b(a) ("[A]ny consumer reporting agency may furnish a consumer report under the following circumstances and no other . . ."); Right to Financial Privacy Act, 12 U. S. C. §3403(a) ("No financial institution, or officer, employees, or agent of a financial institution, may provide to any Government authority access to or copies of, or the information contained in, the financial records of any customer except in accordance with the provisions of this chapter"); Patient Safety and Quality Improvement Act, 42 U. S. C. §299b–22(b) ("Notwithstanding any other provision of Federal, State, or local law, and subject to subsection (c) of this section, patient safety work product shall be confidential and shall not be disclosed"); Cable Act, 47 U. S. C. §551(c)(1) ("[A] cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the sub-

It would be especially strange to hold that the Telecommunication Act's confidentiality provision confers a property right when the Act creates an express exception for any disclosure of records that is "required by law." 47 U. S. C. §222(c)(1). So not only does Carpenter lack "'the most essential and beneficial'" of the "'constituent elements'" of property, *Dickman* v. *Commissioner*, 465 U. S. 330, 336 (1984)—*i.e.*, the right to use the property to the exclusion of others—but he cannot even exclude the party he would most like to keep out, namely, the Government.[5]

For all these reasons, there is no plausible ground for maintaining that the information at issue here represents Carpenter's "papers" or "effects."[6]

---

scriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator").

[5] Carpenter also cannot argue that he owns the cell-site records merely because they fall into the category of records referred to as "customer proprietary network information." 47 U. S. C. §222(c). Even assuming labels alone can confer property rights, nothing in this particular label indicates whether the "information" is "proprietary" to the "customer" or to the provider of the "network." At best, the phrase "customer proprietary network information" is ambiguous, and context makes clear that it refers to the *provider*'s information. The Telecommunications Act defines the term to include all "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship." 47 U. S. C. §222(h)(1)(A). For Carpenter to be right, he must own not only the cell-site records in this case, but also records relating to, for example, the "technical configuration" of his subscribed service—records that presumably include such intensely personal and private information as transmission wavelengths, transport protocols, and link layer system configurations.

[6] Thus, this is not a case in which someone has entrusted papers that he or she owns to the safekeeping of another, and it does not involve a bailment. Cf. *post*, at 14 (GORSUCH, J., dissenting).

B

In the days when this Court followed an exclusively property-based approach to the Fourth Amendment, the distinction between an individual's Fourth Amendment rights and those of a third party was clear cut. We first asked whether the object of the search—say, a house, papers, or effects—belonged to the defendant, and, if it did, whether the Government had committed a "trespass" in acquiring the evidence at issue. *Jones*, 565 U. S., at 411, n. 8.

When the Court held in *Katz* that "property rights are not the sole measure of Fourth Amendment violations," *Soldal* v. *Cook County*, 506 U. S. 56, 64 (1992), the sharp boundary between personal and third-party rights was tested. Under *Katz*, a party may invoke the Fourth Amendment whenever law enforcement officers violate the party's "justifiable" or "reasonable" expectation of privacy. See 389 U. S., at 353; see also *id.*, at 361 (Harlan, J., concurring) (applying the Fourth Amendment where "a person [has] exhibited an actual (subjective) expectation of privacy" and where that "expectation [is] one that society is prepared to recognize as 'reasonable'"). Thus freed from the limitations imposed by property law, parties began to argue that they had a reasonable expectation of privacy in items owned by others. After all, if a trusted third party took care not to disclose information about the person in question, that person might well have a reasonable expectation that the information would not be revealed.

Efforts to claim Fourth Amendment protection against searches of the papers and effects of others came to a head in *Miller*, 425 U. S. 435, where the defendant sought the suppression of two banks' microfilm copies of his checks, deposit slips, and other records. The defendant did not claim that he owned these documents, but he nonetheless argued that "analysis of ownership, property rights and possessory interests in the determination of Fourth

Amendment rights ha[d] been severely impeached" by *Katz* and other recent cases. See Brief for Respondent in *United States* v. *Miller*, O. T. 1975, No. 74–1179, p. 6. Turning to *Katz*, he then argued that he had a reasonable expectation of privacy in the banks' records regarding his accounts. Brief for Respondent in No. 74–1179, at 6; see also *Miller*, *supra*, at 442–443.

Acceptance of this argument would have flown in the face of the Fourth Amendment's text, and the Court rejected that development. Because Miller gave up "dominion and control" of the relevant information to his bank, *Rakas,* 439 U. S., at 149, the Court ruled that he lost any protected Fourth Amendment interest in that information. See *Miller*, *supra*, at 442–443. Later, in *Smith* v. *Maryland*, 442 U. S. 735, 745 (1979), the Court reached a similar conclusion regarding a telephone company's records of a customer's calls. As JUSTICE KENNEDY concludes, *Miller* and *Smith* are thus best understood as placing "necessary limits on the ability of individuals to assert Fourth Amendment interests in property to which they lack a 'requisite connection.'" *Ante*, at 8.

The same is true here, where Carpenter indisputably lacks any meaningful property-based connection to the cell-site records owned by his provider. Because the records are not Carpenter's in any sense, Carpenter may not seek to use the Fourth Amendment to exclude them.

By holding otherwise, the Court effectively allows Carpenter to object to the "search" of a third party's property, not recognizing the revolutionary nature of this change. The Court seems to think that *Miller* and *Smith* invented a new "doctrine"—"the third-party doctrine"—and the Court refuses to "extend" this product of the 1970's to a new age of digital communications. *Ante*, at 11, 17. But the Court fundamentally misunderstands the role of *Miller* and *Smith*. Those decisions did not forge a new doctrine; instead, they rejected an argument that would have

disregarded the clear text of the Fourth Amendment and a formidable body of precedent.

In the end, the Court never explains how its decision can be squared with the fact that the Fourth Amendment protects only "[t]he right of the people to be secure in *their* persons, houses, papers, and effects." (Emphasis added.)

* * *

Although the majority professes a desire not to "'embarrass the future,'" *ante*, at 18, we can guess where today's decision will lead.

One possibility is that the broad principles that the Court seems to embrace will be applied across the board. All subpoenas *duces tecum* and all other orders compelling the production of documents will require a demonstration of probable cause, and individuals will be able to claim a protected Fourth Amendment interest in any sensitive personal information about them that is collected and owned by third parties. Those would be revolutionary developments indeed.

The other possibility is that this Court will face the embarrassment of explaining in case after case that the principles on which today's decision rests are subject to all sorts of qualifications and limitations that have not yet been discovered. If we take this latter course, we will inevitably end up "mak[ing] a crazy quilt of the Fourth Amendment." *Smith*, *supra*, at 745.

All of this is unnecessary. In the Stored Communications Act, Congress addressed the specific problem at issue in this case. The Act restricts the misuse of cell-site records by cell service providers, something that the Fourth Amendment cannot do. The Act also goes beyond current Fourth Amendment case law in restricting access by law enforcement. It permits law enforcement officers to acquire cell-site records only if they meet a heightened standard and obtain a court order. If the American people

now think that the Act is inadequate or needs updating, they can turn to their elected representatives to adopt more protective provisions. Because the collection and storage of cell-site records affects nearly every American, it is unlikely that the question whether the current law requires strengthening will escape Congress's notice.

Legislation is much preferable to the development of an entirely new body of Fourth Amendment caselaw for many reasons, including the enormous complexity of the subject, the need to respond to rapidly changing technology, and the Fourth Amendment's limited scope. The Fourth Amendment restricts the conduct of the Federal Government and the States; it does not apply to private actors. But today, some of the greatest threats to individual privacy may come from powerful private companies that collect and sometimes misuse vast quantities of data about the lives of ordinary Americans. If today's decision encourages the public to think that this Court can protect them from this looming threat to their privacy, the decision will mislead as well as disrupt. And if holding a provision of the Stored Communications Act to be unconstitutional dissuades Congress from further legislation in this field, the goal of protecting privacy will be greatly disserved.

The desire to make a statement about privacy in the digital age does not justify the consequences that today's decision is likely to produce.

SUPREME COURT OF THE UNITED STATES

No. 16–402

TIMOTHY IVORY CARPENTER, PETITIONER *v.* UNITED STATES

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

[June 22, 2018]

JUSTICE GORSUCH, dissenting.

In the late 1960s this Court suggested for the first time that a search triggering the Fourth Amendment occurs when the government violates an "expectation of privacy" that "society is prepared to recognize as 'reasonable.'" *Katz* v. *United States*, 389 U. S. 347, 361 (1967) (Harlan, J., concurring). Then, in a pair of decisions in the 1970s applying the *Katz* test, the Court held that a "reasonable expectation of privacy" *doesn't* attach to information shared with "third parties." See *Smith* v. *Maryland*, 442 U. S. 735, 743–744 (1979); *United States* v. *Miller*, 425 U. S. 435, 443 (1976). By these steps, the Court came to conclude, the Constitution does nothing to limit investigators from searching records you've entrusted to your bank, accountant, and maybe even your doctor.

What's left of the Fourth Amendment? Today we use the Internet to do most everything. Smartphones make it easy to keep a calendar, correspond with friends, make calls, conduct banking, and even watch the game. Countless Internet companies maintain records about us and, increasingly, *for* us. Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers. *Smith* and *Miller* teach that the police can review all of this material, on the theory that no one reasonably

expects any of it will be kept private. But no one believes that, if they ever did.

What to do? It seems to me we could respond in at least three ways. The first is to ignore the problem, maintain *Smith* and *Miller*, and live with the consequences. If the confluence of these decisions and modern technology means our Fourth Amendment rights are reduced to nearly nothing, so be it. The second choice is to set *Smith* and *Miller* aside and try again using the *Katz* "reasonable expectation of privacy" jurisprudence that produced them. The third is to look for answers elsewhere.

*

Start with the first option. *Smith* held that the government's use of a pen register to record the numbers people dial on their phones doesn't infringe a reasonable expectation of privacy because that information is freely disclosed to the third party phone company. 442 U. S., at 743–744. *Miller* held that a bank account holder enjoys no reasonable expectation of privacy in the bank's records of his account activity. That's true, the Court reasoned, "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." 425 U. S., at 443. 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. See *ante,* at 10–18. But as the Sixth Circuit recognized and JUSTICE KENNEDY explains, no balancing test of this kind can be found in *Smith* and *Miller*. See *ante*, at 16 (dissenting opinion). 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.

The problem isn't with the Sixth Circuit's application of *Smith* and *Miller* but with the cases themselves. Can the government demand a copy of all your e-mails from Google or Microsoft without implicating your Fourth Amendment rights? Can it secure your DNA from 23andMe without a warrant or probable cause? *Smith* and *Miller* say yes it can—at least without running afoul of *Katz*. But that result strikes most lawyers and judges today—me included—as pretty unlikely. In the years since its adoption, countless scholars, too, have come to conclude that the "third-party doctrine is not only wrong, but horribly wrong." Kerr, The Case for the Third-Party Doctrine, 107 Mich. L. Rev. 561, 563, n. 5, 564 (2009) (collecting criticisms but defending the doctrine (footnotes omitted)). The reasons are obvious. "As an empirical statement about subjective expectations of privacy," the doctrine is "quite dubious." Baude & Stern, The Positive Law Model of the Fourth Amendment, 129 Harv. L. Rev. 1821, 1872 (2016). People often *do* reasonably expect that information they entrust to third parties, especially information subject to confidentiality agreements, will be kept private. Meanwhile, if the third party doctrine is supposed to represent a normative assessment of when a person should expect privacy, the notion that the answer might be "never" seems a pretty unattractive societal prescription. *Ibid.*

What, then, is the explanation for our third party doctrine? The truth is, the Court has never offered a persuasive justification. The Court has said that by conveying information to a third party you "'assum[e] the risk'" it will be revealed to the police and therefore lack a reason-

able expectation of privacy in it. *Smith*, *supra,* at 744. But assumption of risk doctrine developed in tort law. It generally applies when "by contract or otherwise [one] expressly agrees to accept a risk of harm" or impliedly does so by "manifest[ing] his willingness to accept" that risk and thereby "take[s] his chances as to harm which may result from it." Restatement (Second) of Torts §§496B, 496C(1), and Comment *b* (1965); see also 1 D. Dobbs, P. Hayden, & E. Bublick, Law of Torts §§235–236, pp. 841–850 (2d ed. 2017). That rationale has little play in this context. Suppose I entrust a friend with a letter and he promises to keep it secret until he delivers it to an intended recipient. In what sense have I agreed to bear the risk that he will turn around, break his promise, and spill its contents to someone else? More confusing still, what have I done to "manifest my willingness to accept" the risk that the government will pry the document from my friend and read it *without* his consent?

One possible answer concerns knowledge. I know that my friend *might* break his promise, or that the government *might* have some reason to search the papers in his possession. But knowing about a risk doesn't mean you assume responsibility for it. Whenever you walk down the sidewalk you know a car may negligently or recklessly veer off and hit you, but that hardly means you accept the consequences and absolve the driver of any damage he may do to you. Epstein, Privacy and the Third Hand: Lessons From the Common Law of Reasonable Expectations, 24 Berkeley Tech. L. J. 1199, 1204 (2009); see W. Keeton, D. Dobbs, R. Keeton, & D. Owen, Prosser & Keeton on Law of Torts 490 (5th ed. 1984).

Some have suggested the third party doctrine is better understood to rest on consent than assumption of risk. "So long as a person knows that they are disclosing information to a third party," the argument goes, "their choice to do so is voluntary and the consent valid." Kerr, *supra,*

at 588. I confess I still don't see it. Consenting to give a third party access to private papers that remain my property is not the same thing as consenting to a *search of those papers by the government.* Perhaps there are exceptions, like when the third party is an undercover government agent. See Murphy, The Case Against the Case Against the Third-Party Doctrine: A Response to Epstein and Kerr, 24 Berkeley Tech. L. J. 1239, 1252 (2009); cf. *Hoffa* v. *United States*, 385 U. S. 293 (1966). But otherwise this conception of consent appears to be just assumption of risk relabeled—you've "consented" to whatever risks are foreseeable.

Another justification sometimes offered for third party doctrine is clarity. You (and the police) know exactly how much protection you have in information confided to others: none. As rules go, "the king always wins" is admirably clear. But the opposite rule would be clear too: Third party disclosures *never* diminish Fourth Amendment protection (call it "the king always loses"). So clarity alone cannot justify the third party doctrine.

In the end, what do *Smith* and *Miller* add up to? A doubtful application of *Katz* that lets the government search almost whatever it wants whenever it wants. The Sixth Circuit had to follow that rule and faithfully did just that, but it's not clear why we should.

*

There's a second option. What if we dropped *Smith* and *Miller*'s third party doctrine and retreated to the root *Katz* question whether there is a "reasonable expectation of privacy" in data held by third parties? Rather than solve the problem with the third party doctrine, I worry this option only risks returning us to its source: After all, it was *Katz* that produced *Smith* and *Miller* in the first place.

Katz's problems start with the text and original under-

standing of the Fourth Amendment, as JUSTICE THOMAS thoughtfully explains today. *Ante,* at 5–17 (dissenting opinion). The Amendment's protections do not depend on the breach of some abstract "expectation of privacy" whose contours are left to the judicial imagination. Much more concretely, it protects your "person," and your "houses, papers, and effects." Nor does your right to bring a Fourth Amendment claim depend on whether a judge happens to agree that your subjective expectation to privacy is a "reasonable" one. Under its plain terms, the Amendment grants you the right to invoke its guarantees whenever one of your protected things (your person, your house, your papers, or your effects) is unreasonably searched or seized. Period.

History too holds problems for *Katz*. Little like it can be found in the law that led to the adoption of the Fourth Amendment or in this Court's jurisprudence until the late 1960s. The Fourth Amendment came about in response to a trio of 18th century cases "well known to the men who wrote and ratified the Bill of Rights, [and] famous throughout the colonial population." Stuntz, The Substantive Origins of Criminal Procedure, 105 Yale L. J. 393, 397 (1995). The first two were English cases invalidating the Crown's use of general warrants to enter homes and search papers. *Entick* v. *Carrington*, 19 How. St. Tr. 1029 (K. B. 1765); *Wilkes* v. *Wood*, 19 How. St. Tr. 1153 (K. B. 1763); see W. Cuddihy, The Fourth Amendment: Origins and Original Meaning 439–487 (2009); *Boyd* v. *United States*, 116 U. S. 616, 625–630 (1886). The third was American: the Boston Writs of Assistance Case, which sparked colonial outrage at the use of writs permitting government agents to enter houses and business, breaking open doors and chests along the way, to conduct searches and seizures—and to force third parties to help them. Stuntz, *supra,* at 404–409; M. Smith, The Writs of Assistance Case (1978). No doubt the colonial outrage engen-

dered by these cases rested in part on the government's intrusion upon privacy. But the framers chose not to protect privacy in some ethereal way dependent on judicial intuitions. They chose instead to protect privacy in particular places and things—"persons, houses, papers, and effects"—and against particular threats—"unreasonable" governmental "searches and seizures." See *Entick*, *supra,* at 1066 ("Papers are the owner's goods and chattels; they are his dearest property; and so far from enduring a seizure, that they will hardly bear an inspection"); see also *ante,* at 1–21 (THOMAS, J., dissenting).

Even taken on its own terms, *Katz* has never been sufficiently justified. In fact, we still don't even know what its "reasonable expectation of privacy" test *is*. Is it supposed to pose an empirical question (what privacy expectations do people *actually* have) or a normative one (what expectations *should* they have)? Either way brings problems. If the test is supposed to be an empirical one, it's unclear why judges rather than legislators should conduct it. Legislators are responsive to their constituents and have institutional resources designed to help them discern and enact majoritarian preferences. Politically insulated judges come armed with only the attorneys' briefs, a few law clerks, and their own idiosyncratic experiences. They are hardly the representative group you'd expect (or want) to be making empirical judgments for hundreds of millions of people. Unsurprisingly, too, judicial judgments often fail to reflect public views. See Slobogin & Schumacher, Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society," 42 Duke L. J. 727, 732, 740–742 (1993). Consider just one example. Our cases insist that the seriousness of the offense being investigated does *not* reduce Fourth Amendment protection. *Mincey* v. *Arizona*, 437 U. S. 385, 393–394 (1978). Yet scholars suggest that most people *are* more tolerant of

police intrusions when they investigate more serious crimes. See Blumenthal, Adya, & Mogle, The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy," 11 U. Pa. J. Const. L. 331, 352–353 (2009). And I very much doubt that this Court would be willing to adjust its *Katz* cases to reflect these findings even if it believed them.

Maybe, then, the *Katz* test should be conceived as a normative question. But if that's the case, why (again) do judges, rather than legislators, get to determine whether society *should be* prepared to recognize an expectation of privacy as legitimate? Deciding what privacy interests *should be* recognized often calls for a pure policy choice, many times between incommensurable goods—between the value of privacy in a particular setting and society's interest in combating crime. Answering questions like that calls for the exercise of raw political will belonging to legislatures, not the legal judgment proper to courts. See The Federalist No. 78, p. 465 (C. Rossiter ed. 1961) (A. Hamilton). When judges abandon legal judgment for political will we not only risk decisions where "reasonable expectations of privacy" come to bear "an uncanny resemblance to those expectations of privacy" shared by Members of this Court. *Minnesota* v. *Carter*, 525 U. S. 83, 97 (1998) (Scalia, J., concurring). We also risk undermining public confidence in the courts themselves.

My concerns about *Katz* come with a caveat. *Sometimes*, I accept, judges may be able to discern and describe existing societal norms. See, *e.g., Florida* v. *Jardines*, 569 U. S. 1, 8 (2013) (inferring a license to enter on private property from the "'habits of the country'" (quoting *McKee* v. *Gratz*, 260 U. S. 127, 136 (1922))); Sachs, Finding Law, 107 Cal. L. Rev. (forthcoming 2019), online at https://ssrn.com/abstract=3064443 (as last visited June 19, 2018). That is particularly true when the judge looks to positive law rather than intuition for guidance on social norms. See

Byrd v. *United States,* 584 U. S. ___, ___–___ (2018) (slip op., at 7–9) ("general property-based concept[s] guid[e] the resolution of this case"). So there may be *some* occasions where *Katz* is capable of principled application—though it may simply wind up approximating the more traditional option I will discuss in a moment. Sometimes it may also be possible to apply *Katz* by analogizing from precedent when the line between an existing case and a new fact pattern is short and direct. But so far this Court has declined to tie itself to any significant restraints like these. See *ante,* at 5, n. 1 ("[W]hile property rights are often informative, our cases by no means suggest that such an interest is 'fundamental' or 'dispositive' in determining which expectations of privacy are legitimate").

As a result, *Katz* has yielded an often unpredictable—and sometimes unbelievable—jurisprudence. *Smith* and *Miller* are only two examples; there are many others. Take *Florida* v. *Riley*, 488 U. S. 445 (1989), which says that a police helicopter hovering 400 feet above a person's property invades no reasonable expectation of privacy. Try that one out on your neighbors. Or *California* v. *Greenwood*, 486 U. S. 35 (1988), which holds that a person has no reasonable expectation of privacy in the garbage he puts out for collection. In that case, the Court said that the homeowners forfeited their privacy interests because "[i]t is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public." *Id.*, at 40 (footnotes omitted). But the habits of raccoons don't prove much about the habits of the country. I doubt, too, that most people spotting a neighbor rummaging through their garbage would think they lacked reasonable grounds to confront the rummager. Making the decision all the stranger, California state law expressly *protected* a homeowner's property rights in discarded trash. *Id.*, at 43. Yet rather than defer to that

as evidence of the people's habits and reasonable expectations of privacy, the Court substituted its own curious judgment.

Resorting to *Katz* in data privacy cases threatens more of the same. Just consider. The Court today says that judges should use *Katz*'s reasonable expectation of privacy test to decide what Fourth Amendment rights people have in cell-site location information, explaining that "no single rubric definitively resolves which expectations of privacy are entitled to protection." *Ante,* at 5. But then it offers a twist. Lower courts should be sure to add two special principles to their *Katz* calculus: the need to avoid "arbitrary power" and the importance of "plac[ing] obstacles in the way of a too permeating police surveillance." *Ante,* at 6 (internal quotation marks omitted). While surely laudable, these principles don't offer lower courts much guidance. The Court does not tell us, for example, how far to carry either principle or how to weigh them against the legitimate needs of law enforcement. At what point does access to electronic data amount to "arbitrary" authority? When does police surveillance become "too permeating"? And what sort of "obstacles" should judges "place" in law enforcement's path when it does? We simply do not know.

The Court's application of these principles supplies little more direction. The Court declines to say whether there is any sufficiently limited period of time "for which the Government may obtain an individual's historical [location information] free from Fourth Amendment scrutiny." *Ante,* at 11, n. 3; see *ante,* at 11–15. But then it tells us that access to seven days' worth of information *does* trigger Fourth Amendment scrutiny—even though here the carrier "produced only two days of records." *Ante,* at 11, n. 3. Why is the relevant fact the seven days of information the government *asked for* instead of the two days of information the government *actually saw*? Why seven days instead of ten or three or one? And in what possible sense

did the government "search" five days' worth of location information it was never even sent? We do not know.

Later still, the Court adds that it can't say whether the Fourth Amendment is triggered when the government collects "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)." *Ante,* at 17–18. But what distinguishes historical data from real-time data, or seven days of a single person's data from a download of *everyone*'s data over some indefinite period of time? Why isn't a tower dump the *paradigmatic* example of "too permeating police surveillance" and a dangerous tool of "arbitrary" authority—the touchstones of the majority's modified *Katz* analysis? On what possible basis could such mass data collection survive the Court's test while collecting a single person's data does not? Here again we are left to guess. At the same time, though, the Court offers some firm assurances. It tells us its decision does *not* "call into question conventional surveillance techniques and tools, such as security cameras." *Ibid.* That, however, just raises more questions for lower courts to sort out about what techniques qualify as "conventional" and why those techniques would be okay *even if* they lead to "permeating police surveillance" or "arbitrary police power."

Nor is this the end of it. After finding a reasonable expectation of privacy, the Court says there's still more work to do. Courts must determine whether to "extend" *Smith* and *Miller* to the circumstances before them. *Ante,* at 11, 15–17. So apparently *Smith* and *Miller* aren't quite left for dead; they just no longer have the clear reach they once did. How do we measure their new reach? The Court says courts now must conduct a *second Katz*-like balancing inquiry, asking whether the fact of disclosure to a third party outweighs privacy interests in the "category of information" so disclosed. *Ante,* at 13, 15–16. But how are lower courts supposed to weigh these radically different

interests? Or assign values to different categories of information? All we know is that historical cell-site location information (for seven days, anyway) escapes *Smith* and *Miller*'s shorn grasp, while a lifetime of bank or phone records does not. As to any other kind of information, lower courts will have to stay tuned.

In the end, our lower court colleagues are left with two amorphous balancing tests, a series of weighty and incommensurable principles to consider in them, and a few illustrative examples that seem little more than the product of judicial intuition. In the Court's defense, though, we have arrived at this strange place not because the Court has misunderstood *Katz*. Far from it. We have arrived here because this is where *Katz* inevitably leads.

*

There is another way. From the founding until the 1960s, the right to assert a Fourth Amendment claim didn't depend on your ability to appeal to a judge's personal sensibilities about the "reasonableness" of your expectations or privacy. It was tied to the law. *Jardines*, 569 U. S., at 11; *United States* v. *Jones*, 565 U. S. 400, 405 (2012). The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures." True to those words and their original understanding, the traditional approach asked if a house, paper or effect was *yours* under law. No more was needed to trigger the Fourth Amendment. Though now often lost in *Katz*'s shadow, this traditional understanding persists. *Katz* only "supplements, rather than displaces the traditional property-based understanding of the Fourth Amendment." *Byrd*, 584 U. S., at ___ (slip op., at 7) (internal quotation marks omitted); *Jardines*, *supra,* at 11 (same); *Soldal* v. *Cook County*, 506 U. S. 56, 64 (1992) (*Katz* did not "snuf[f] out the previously recognized protection for property under

the Fourth Amendment").

Beyond its provenance in the text and original understanding of the Amendment, this traditional approach comes with other advantages. Judges are supposed to decide cases based on "democratically legitimate sources of law"—like positive law or analogies to items protected by the enacted Constitution—rather than "their own biases or personal policy preferences." Pettys, Judicial Discretion in Constitutional Cases, 26 J. L. & Pol. 123, 127 (2011). A Fourth Amendment model based on positive legal rights "carves out significant room for legislative participation in the Fourth Amendment context," too, by asking judges to consult what the people's representatives have to say about their rights. Baude & Stern, 129 Harv. L. Rev., at 1852. Nor is this approach hobbled by *Smith* and *Miller*, for those cases are just *limitations* on *Katz*, addressing only the question whether individuals have a reasonable expectation of privacy in materials they share with third parties. Under this more traditional approach, Fourth Amendment protections for your papers and effects do not automatically disappear just because you share them with third parties.

Given the prominence *Katz* has claimed in our doctrine, American courts are pretty rusty at applying the traditional approach to the Fourth Amendment. We know that if a house, paper, or effect is yours, you have a Fourth Amendment interest in its protection. But what kind of legal interest is sufficient to make something *yours*? And what source of law determines that? Current positive law? The common law at 1791, extended by analogy to modern times? Both? See *Byrd*, *supra*, at ___–___ (slip op., at 1–2) (THOMAS, J., concurring); cf. Re, The Positive Law Floor, 129 Harv. L. Rev. Forum 313 (2016). Much work is needed to revitalize this area and answer these questions. I do not begin to claim all the answers today, but (unlike with *Katz*) at least I have a pretty good idea

what the questions *are*. And it seems to me a few things can be said.

First, the fact that a third party has access to or possession of your papers and effects does not necessarily eliminate your interest in them. Ever hand a private document to a friend to be returned? Toss your keys to a valet at a restaurant? Ask your neighbor to look after your dog while you travel? You would not expect the friend to share the document with others; the valet to lend your car to his buddy; or the neighbor to put Fido up for adoption. Entrusting your stuff to others is a *bailment*. A bailment is the "delivery of personal property by one person (the *bailor*) to another (the *bailee*) who holds the property for a certain purpose." Black's Law Dictionary 169 (10th ed. 2014); J. Story, Commentaries on the Law of Bailments §2, p. 2 (1832) ("a bailment is a delivery of a thing in trust for some special object or purpose, and upon a contract, expressed or implied, to conform to the object or purpose of the trust"). A bailee normally owes a legal duty to keep the item safe, according to the terms of the parties' contract if they have one, and according to the "implication[s] from their conduct" if they don't. 8 C. J. S., Bailments §36, pp. 468–469 (2017). A bailee who uses the item in a different way than he's supposed to, or against the bailor's instructions, is liable for conversion. *Id.*, §43, at 481; see *Goad* v. *Harris*, 207 Ala. 357, 92 So. 546, (1922); *Knight* v. *Seney*, 290 Ill. 11, 17, 124 N. E. 813, 815–816 (1919); *Baxter* v. *Woodward*, 191 Mich. 379, 385, 158 N. W. 137, 139 (1916). This approach is quite different from *Smith* and *Miller*'s (counter)-intuitive approach to reasonable expectations of privacy; where those cases extinguish Fourth Amendment interests once records are given to a third party, property law may preserve them.

Our Fourth Amendment jurisprudence already reflects this truth. In *Ex parte Jackson*, 96 U. S. 727 (1878), this Court held that sealed letters placed in the mail are "as

fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles." *Id.,* at 733. The reason, drawn from the Fourth Amendment's text, was that "[t]he constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to *their papers*, thus closed against inspection, *wherever they may be*." *Ibid.* (emphasis added). It did not matter that letters were bailed to a third party (the government, no less). The sender enjoyed the same Fourth Amendment protection as he does "when papers are subjected to search in one's own household." *Ibid.*

These ancient principles may help us address modern data cases too. Just because you entrust your data—in some cases, your modern-day papers and effects—to a third party may not mean you lose any Fourth Amendment interest in its contents. Whatever may be left of *Smith* and *Miller*, few doubt that e-mail should be treated much like the traditional mail it has largely supplanted—as a bailment in which the owner retains a vital and protected legal interest. See *ante,* at 13 (KENNEDY, J., dissenting) (noting that enhanced Fourth Amendment protection may apply when the "modern-day equivalents of an individual's own 'papers' or 'effects' . . . are held by a third party" through "bailment"); *ante,* at 23, n. 6 (ALITO, J., dissenting) (reserving the question whether Fourth Amendment protection may apply in the case of "bailment" or when "someone has entrusted papers he or she owns . . . to the safekeeping of another"); *United States* v. *Warshak*, 631 F. 3d 266, 285–286 (CA6 2010) (relying on an analogy to *Jackson* to extend Fourth Amendment protection to e-mail held by a third party service provider).

Second, I doubt that complete ownership or exclusive control of property is always a necessary condition to the assertion of a Fourth Amendment right. Where houses

are concerned, for example, individuals can enjoy Fourth Amendment protection without fee simple title. Both the text of the Amendment and the common law rule support that conclusion. "People call a house 'their' home when legal title is in the bank, when they rent it, and even when they merely occupy it rent free." *Carter*, 525 U. S., at 95–96 (Scalia, J., concurring). That rule derives from the common law. *Oystead* v. *Shed*, 13 Mass. 520, 523 (1816) (explaining, citing "[t]he very learned judges, *Foster*, *Hale*, and *Coke*," that the law "would be as much disturbed by a forcible entry to arrest a boarder or a servant, who had acquired, by contract, express or implied, a right to enter the house at all times, and to remain in it as long as they please, as if the object were to arrest the master of the house or his children"). That is why tenants and resident family members—though they have no legal title—have standing to complain about searches of the houses in which they live. *Chapman* v. *United States*, 365 U. S. 610, 616–617 (1961), *Bumper* v. *North Carolina*, 391 U. S. 543, 548, n. 11 (1968).

Another point seems equally true: just because you *have* to entrust a third party with your data doesn't necessarily mean you should lose all Fourth Amendment protections in it. Not infrequently one person comes into possession of someone else's property without the owner's consent. Think of the finder of lost goods or the policeman who impounds a car. The law recognizes that the goods and the car still belong to their true owners, for "where a person comes into lawful possession of the personal property of another, even though there is no formal agreement between the property's owner and its possessor, the possessor will become a constructive bailee when justice so requires." *Christensen* v. *Hoover*, 643 P. 2d 525, 529 (Colo. 1982) (en banc); Laidlaw, Principles of Bailment, 16 Cornell L. Q. 286 (1931). At least some of this Court's decisions have already suggested that use of technology is

functionally compelled by the demands of modern life, and in that way the fact that we store data with third parties may amount to a sort of involuntary bailment too. See *ante,* at 12–13 (majority opinion); *Riley* v. *California*, 573 U. S. ___, ___ (2014) (slip op., at 9).

Third, positive law may help provide detailed guidance on evolving technologies without resort to judicial intuition. State (or sometimes federal) law often creates rights in both tangible and intangible things. See *Ruckelshaus* v. *Monsanto Co.*, 467 U. S. 986, 1001 (1984). In the context of the Takings Clause we often ask whether those state-created rights are sufficient to make something someone's property for constitutional purposes. See *id.,* at 1001–1003; *Louisville Joint Stock Land Bank* v. *Radford*, 295 U. S. 555, 590–595 (1935). A similar inquiry may be appropriate for the Fourth Amendment. Both the States and federal government are actively legislating in the area of third party data storage and the rights users enjoy. See, *e.g.,* Stored Communications Act, 18 U. S. C. §2701 *et seq.*; Tex. Prop. Code Ann. §111.004(12) (West 2017) (defining "[p]roperty" to include "property held in any digital or electronic medium"). State courts are busy expounding common law property principles in this area as well. *E.g., Ajemian* v. *Yahoo!, Inc.*, 478 Mass. 169, 170, 84 N. E. 3d 766, 768 (2017) (e-mail account is a "form of property often referred to as a 'digital asset'"); *Eysoldt* v. *ProScan Imaging*, 194 Ohio App. 3d 630, 638, 2011–Ohio–2359, 957 N. E. 2d 780, 786 (2011) (permitting action for conversion of web account as intangible property). If state legislators or state courts say that a digital record has the attributes that normally make something property, that may supply a sounder basis for judicial decisionmaking than judicial guesswork about societal expectations.

Fourth, while positive law may help establish a person's Fourth Amendment interest there may be some circumstances where positive law cannot be used to defeat it.

Ex parte Jackson reflects that understanding. There this Court said that "[n]o law of Congress" could authorize letter carriers "to invade the secrecy of letters." 96 U. S., at 733. So the post office couldn't impose a regulation dictating that those mailing letters surrender all legal interests in them once they're deposited in a mailbox. If that is right, *Jackson* suggests the existence of a constitutional floor below which Fourth Amendment rights may not descend. Legislatures cannot pass laws declaring your house or papers to be your property except to the extent the police wish to search them without cause. As the Court has previously explained, "we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Jones*, 565 U. S., at 406 (quoting *Kyllo* v. *United States*, 533 U. S. 27, 34 (2001)). Nor does this mean protecting only the specific rights known at the founding; it means protecting their modern analogues too. So, for example, while thermal imaging was unknown in 1791, this Court has recognized that using that technology to look inside a home constitutes a Fourth Amendment "search" of that "home" no less than a physical inspection might. *Id.,* at 40.

Fifth, this constitutional floor may, in some instances, bar efforts to circumvent the Fourth Amendment's protection through the use of subpoenas. No one thinks the government can evade *Jackson*'s prohibition on opening sealed letters without a warrant simply by issuing a subpoena to a postmaster for "all letters sent by John Smith" or, worse, "all letters sent by John Smith concerning a particular transaction." So the question courts will confront will be this: What other kinds of records are sufficiently similar to letters in the mail that the same rule should apply?

It may be that, as an original matter, a subpoena requiring the recipient to produce records wasn't thought of as a

"search or seizure" by the government implicating the Fourth Amendment, see *ante,* at 2–12 (opinion of ALITO, J.), but instead as an act of compelled self-incrimination implicating the Fifth Amendment, see *United States* v. *Hubbell*, 530 U. S. 27, 49–55 (2000) (THOMAS, J., dissenting); Nagareda, Compulsion "To Be a Witness" and the Resurrection of Boyd, 74 N. Y. U. L. Rev. 1575, 1619, and n. 172 (1999). But the common law of searches and seizures does not appear to have confronted a case where private documents equivalent to a mailed letter were entrusted to a bailee and then subpoenaed. As a result, "[t]he common-law rule regarding subpoenas for documents held by third parties entrusted with information from the target is . . . unknown and perhaps unknowable." Dripps, Perspectives on The Fourth Amendment Forty Years Later: Toward the Realization of an Inclusive Regulatory Model, 100 Minn. L. Rev. 1885, 1922 (2016). Given that (perhaps insoluble) uncertainty, I am content to adhere to *Jackson* and its implications for now.

To be sure, we must be wary of returning to the doctrine of *Boyd* v. *United States*, 116 U. S. 616. *Boyd* invoked the Fourth Amendment to restrict the use of subpoenas even for ordinary business records and, as JUSTICE ALITO notes, eventually proved unworkable. See *ante,* at 13 (dissenting opinion); 3 W. LaFave, J. Israel, N. King, & O. Kerr, Criminal Procedure §8.7(a), pp. 185–187 (4th ed. 2015). But if we were to overthrow *Jackson* too and deny Fourth Amendment protection to *any* subpoenaed materials, we would do well to reconsider the scope of the Fifth Amendment while we're at it. Our precedents treat the right against self-incrimination as applicable only to testimony, not the production of incriminating evidence. See *Fisher* v. *United States*, 425 U. S. 391, 401 (1976). But there is substantial evidence that the privilege against self-incrimination was also originally understood to protect a person from being forced to turn over potentially incrimi-

nating evidence. Nagareda, *supra,* at 1605–1623; *Rex* v. *Purnell*, 96 Eng. Rep. 20 (K. B. 1748); Slobogin, Privacy at Risk 145 (2007).

*

What does all this mean for the case before us? To start, 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 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.

Our case offers a cautionary example. It seems to me entirely possible a person's cell-site data could qualify as *his* papers or effects under existing law. Yes, the telephone carrier holds the information. But 47 U. S. C. §222 designates a customer's cell-site location information as "customer proprietary network information" (CPNI), §222(h)(1)(A), and gives customers certain rights to control use of and access to CPNI about themselves. The statute generally forbids a carrier to "use, disclose, or permit access to individually identifiable" CPNI without the customer's consent, except as needed to provide the customer's telecommunications services. §222(c)(1). It also

requires the carrier to disclose CPNI "upon affirmative written request by the customer, to any person designated by the customer." §222(c)(2). Congress even afforded customers a private cause of action for damages against carriers who violate the Act's terms. §207. Plainly, customers have substantial legal interests in this information, including at least some right to include, exclude, and control its use. Those interests might even rise to the level of a property right.

The problem is that we do not know anything more. Before the district court and court of appeals, Mr. Carpenter pursued only a *Katz* "reasonable expectations" argument. He did not invoke the law of property or any analogies to the common law, either there or in his petition for certiorari. Even in his merits brief before this Court, Mr. Carpenter's discussion of his positive law rights in cell-site data was cursory. He offered no analysis, for example, of what rights state law might provide him in addition to those supplied by §222. In these circumstances, I cannot help but conclude—reluctantly—that Mr. Carpenter forfeited perhaps his most promising line of argument.

Unfortunately, too, this case marks the second time this Term that individuals have forfeited Fourth Amendment arguments based on positive law by failing to preserve them. See *Byrd*, 584 U. S., at ___ (slip op., at 7). Litigants have had fair notice since at least *United States* v. *Jones* (2012) and *Florida* v. *Jardines* (2013) that arguments like these may vindicate Fourth Amendment interests even where *Katz* arguments do not. Yet the arguments have gone unmade, leaving courts to the usual *Katz* handwaving. These omissions do not serve the development of a sound or fully protective Fourth Amendment jurisprudence.

Congressional Research Service
Informing the legislative debate since 1914

Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA)

Richard M. Thompson II
Legislative Attorney

Jared P. Cole
Legislative Attorney

May 19, 2015

Congressional Research Service
7-5700
www.crs.gov
R44036

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA) to both protect the privacy of an individual's electronic communications and provide the government with a means for accessing these communications and related records. Although passed at the infancy of the Internet, the Stored Communications Act (SCA), which is part of ECPA, has been interpreted over the years to cover the content of emails, private Facebook messages, YouTube videos, and so-called metadata, or non-content information, connected to our Internet transactions (e.g., websites visited, to/from and time/date stamps on emails).

The scope of the SCA is determined largely by the entities to which it applies, "electronic communication service" (ECS) providers and "remote computing service" (RCS) providers, as defined in the statute. It does not apply to government access to records held by a party to the communication. The SCA has two core components. First, it creates a broad bar against service providers voluntarily disclosing a customer's communications to the government or others, subject to various exceptions, and second, it establishes procedures under which the government can require a provider to disclose customers' communications or records. As to government access, ECPA utilizes a tiered system with different levels of evidence required depending on whether the provider is an ECS or RCS; whether the data sought is content or non-content; whether the email has been opened; and whether advance notice has been given to the customer.

In recent years, ECPA has faced increased criticism from both the technology and privacy communities that it has outlived its usefulness in the digital era and does not provide adequate privacy safeguards for individuals' electronic communications. In light of these concerns, various reform bills have been introduced in the past several Congresses, with three major reform bills pending in the 114th Congress. The Electronic Communications Privacy Act Amendments Act of 2015 (S. 356, H.R. 283) and the Email Privacy Act (H.R. 699), almost identical in text, would, among other things, place both ECS and RCS providers under the same legal requirement; eliminate the current 180-day rule found in the SCA and require a warrant for emails no matter how long they have been stored or whether they have been opened; and remove the reliance on the definition of "electronic storage," which has confused the lower courts. Additionally, the Online Communications and Geolocation Privacy Act (H.R. 656) would make similar changes to the SCA.

Some federal agencies, most prominently the Securities and Exchange Commission (SEC), which currently rely on their subpoena authority to access electronic communications, have argued that these bills would stymie their ability to conduct investigations as they have no legal authority to obtain a warrant. In response to this concern, both the Email Privacy Act and the ECPA Amendments Act include a rule of construction providing that nothing in these bills should be read to preclude the SEC or any other federal agency from seeking these records directly from a party to the communication, rather than the target's service provider.

Finally, there has been ongoing litigation in the lower federal courts as to ECPA's extraterritorial reach. The Law Enforcement Access to Data Stored Abroad (LEADS) Act (S. 512, H.R. 1174) would require third-party service providers to disclose the contents of U.S persons' electronic communications held overseas upon issuance of a warrant based on probable cause.

Contents

Contacts

Introduction

In 1986, when introducing the Electronic Communications Privacy Act (ECPA), Senator Patrick Leahy observed that the nation's then-existing electronic communications privacy laws were "hopelessly out of date."[1] The Senate Judiciary Committee agreed that the law had "not kept pace with the development of communication and computer technology ... [n]or [had] it kept pace with changes in the structure of the telecommunications industry."[2] Later that year, Congress enacted ECPA, which, at over 25 years old, remains the primary law governing government and private actor access to our stored online communications. It governs, for instance, when the government can demand that Google turn over emails; when social media sites like Facebook must provide private posts; when video-sharing sites like YouTube must provide stored videos; and when cell phone companies must turn over cell location information.

In recent years, ECPA has faced increased criticism from both the technology and privacy communities that it has outlived its usefulness in the digital era and does not provide adequate privacy safeguards for individuals' electronic communications. In light of these concerns, various reform bills have been introduced in the past several Congresses, with three major reform bills pending in the 114th Congress. The Electronic Communications Privacy Act Amendments Act of 2015 (S. 356) and the Email Privacy Act (H.R. 699), almost identical in text, would, among other things, place both ECSs and RCSs under the same legal requirement; eliminate the current 180-day rule found in the Stored Communications Act (SCA) and require a warrant for emails no matter how long they have been stored or whether they have been opened; and eliminate the reliance on the definition of "electronic storage," which has confused the lower courts. Additionally, the Online Communications and Geolocation Privacy Act (H.R. 656) would make similar changes to the SCA.[3]

Some federal agencies, most prominently the Securities and Exchange Commission (SEC), which currently rely on their subpoena authority to access electronic communications, have argued that these bills would stymie their ability to conduct investigations as they lack legal authority to obtain a warrant. In response to this concern, both the Email Privacy Act and the ECPA Amendments Act include a rule of construction providing that nothing in these bills should be read to preclude the SEC or any other federal agency from seeking these records directly from a party to the communication, rather than the target's third-party service provider.

Finally, there has been ongoing litigation in the lower federal courts as to ECPA's extraterritorial reach. The Law Enforcement Access to DATA Stored Abroad (LEADS) Act would require third-party service providers to disclose the contents of U.S persons' electronic communications held overseas upon issuance of a warrant based on probable cause.[4]

This report provides an overview of ECPA reform. It will first outline the background and history of the legal environment prior to ECPA and the problem precipitating ECPA's passage. It will then survey the current legal framework for accessing electronic communications and other non-

[1] 132 Cong. Rec. 14608 (1986).

[2] S. Rept. 99-541, at 2.

[3] H.R. 656, 114th Cong. (2015).

[4] S. 512, 114th Cong. (2015); H.R. 1174, 114th Cong. (2015).

content information from providers, and describe specific types of data accessible under ECPA. Finally, it will explore the various bills that would amend ECPA, including selected legal issues raised by these measures.

Background of ECPA

Before passage of ECPA in 1986, government access to private electronic communications was governed primarily by the Fourth Amendment and the federal wiretap law. In 1967, the Supreme Court issued two landmark Fourth Amendment cases. In *Katz v. United States*, the Court held that the Fourth Amendment's prohibition against "unreasonable searches and seizures" entitles individuals to a reasonable expectation of privacy in their private communications.[5] In *Berger v. New York*, the Court struck down a New York wiretap law that failed to include adequate safeguards for the privacy interests of those whose communications were being "tapped."[6]

One year later, in an effort to regulate wiretapping while also giving law enforcement a lawful means for intercepting telephone conversations, Congress enacted the "Wiretap Act" as Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[7] Title III prohibits the unauthorized interception of wire or oral communications, while simultaneously providing a procedure for law enforcement to conduct such interceptions upon judicial approval.[8] However, Title III only covered the "aural" interception of wire or oral communications—the interception of actual sounds—that are interpreted by hearing, and not sight.[9] This left largely unregulated the transfer of digital communications.[10]

This legal uncertainty as to whether new digital forms of communication would be covered by Title III or other federal law prompted the introduction of the original version of ECPA in 1985.[11] Foreshadowing arguments made by proponents of ECPA reform today, the Senate Judiciary Committee observed at the time that this gap in coverage could stifle American technological innovation, expose law enforcement to liability, allow the erosion of American privacy rights, and jeopardize the admissibility of probative evidence in criminal prosecutions.[12] One year later Congress enacted ECPA.[13]

---

[5] *See* U.S. CONST. amend IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."); Katz v. United States, 389 U.S. 347, 359 (1967).

[6] Berger v. New York, 388 U.S. 41, 63-64 (1967).

[7] Omnibus Crime Control and Safe Streets Act of 1968, P.L. 90-351, 801, 82 Stat. 197, 212.

[8] See 18 U.S.C. § 2511.

[9] *See* United States v. New York Telephone Co., 434 U.S. 159, 166-67 (1977); United States v. Seidlitz, 589 F.2d 152, 157 (4th Cir. 1978) ("The words 'aural acquisition' literally translated mean to come into possession through the sense of hearing.") (quoting Webster's Third New International Dictionary, 1967 ed.)).

[10] *See* OFFICE OF TECHNOLOGY ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 46 (1985).

[11] *Id.* at 21.

[12] S. Rept. 99-541, at 5.

[13] Electronic Communications Privacy Act of 1986, P.L. 99-508, 100 Stat. 1848.

ECPA's Framework

ECPA contains three main titles. Title I updated the Wiretap Act to include not only the interception of oral and wire communications, but also electronic communications.[14] Title III created new rules regulating the use of a pen register, a device that allows users to capture the routing information associated with communications, such as telephone numbers dialed or the to/from address in an email.[15] Title II added Chapter 121 to the *United States Code* entitled "Stored Wire and Electronic Communications and Transactional Records Access," commonly referred to as the Stored Communications Act (SCA).[16] As technology has developed, law enforcement has relied less frequently on real-time interception authorized under the Wiretap Act, and has instead relied on its authority under the SCA—accessing stored electronic communications, such as emails directly from a service provider.[17] This shift explains why reform of ECPA has centered almost entirely on the SCA.

The scope of the SCA is determined largely by the entities to which it applies. First, it does not apply to personal users, but only to providers of an "electronic communication service" (ECS) and a "remote computing service" (RCS).[18] A provider of ECS allows its customers "to send or receive wire or electronic communications."[19] A provider of RCS provides "computer storage or processing services by means of an electronic communication system."[20] Although these definitions can be confusing in the abstract, they make more sense when applied.

The SCA has two core components: (1) a broad prohibition against providers voluntarily sharing customers' communications with the government or others, subject to certain enumerated exceptions,[21] and (2) procedures permitting the government to require the disclosure of customers' communications or records.[22]

As to the first component, under 18 U.S.C. § 2702(a)(1), a provider of ECS to the public "shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage."[23] The importance of the definition of "electronic storage" will be discussed below.[24]

Section 2702(a)(2) states that a provider of RCS to the public shall not knowingly disclose the contents of a communication which is carried or maintained by that service.[25] There are two other conditions that must be met in order for a communication to remain protected under subsection (a)(2). First, the communication must be maintained "on behalf of, and received by means of

[14] *Id*.

[15] *Id.* at 1868.

[16] *Id.* at 1860.

[17] *See* Orin Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373, 394 (2014).

[18] *See* 18 U.S.C. § 2702(a)(1)-(2).

[19] 18 U.S.C. § 2510(15).

[20] *Id.* § 2711(2).

[21] *Id.* § 2702.

[22] *Id.* § 2703.

[23] *Id.* § 2702(a)(1).

[24] *See infra* note 35 and accompanying text.

[25] *Id.* § 2702(a)(2).

electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service."[26] Second, the communication must be maintained "solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing."[27] Although there appears to be little case law interpreting this second condition, it would appear that an RCS which is permitted to access the contents of a communication for purposes other than storage or computer processing—for example, advertising—would not be subject to the prohibition on disclosing the contents of communications.[28] In essence, it acts as an additional exception to nondisclosure.

Section 2702(a)(3) prohibits a provider of ECS or RCS to the public from disclosing a "record or other information pertaining to a subscriber to or customer of such service (not including the contents of a communication covered by paragraph (1) or (2)) to any governmental entity."[29] Note that this rule, which concerns non-content or "metadata," does not apply to nongovernmental, private entities. This permits companies to share non-content information with other private entities, insofar as the SCA is concerned. There may be other federal or state laws, however, which prohibit disclosure of particular classes of information.[30]

Section 2702(b) provides exceptions to the *permissible* disclosure of the *content* of communications covered by the prohibitions in subsection (a), including: to an addressee or intended recipient of a communication, as authorized under Section 2703; as may be necessary incident to the rendition of the service or the protection of the rights of property of the provider of that service; or to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.[31] Section 2702(c) provides similar exceptions for the disclosure of *non-content* information, including as authorized under Section 2703; with the lawful consent of the customer or subscriber; and to any person other than a governmental entity.[32]

The second major component of the SCA is the rules concerning *required* disclosure of customer communications and records. Section 2703 sets up a tiered system with different standards that apply depending on whether an ECS or RCS is holding the record, whether the data sought is content or non-content, whether the email has been opened, and whether advanced notice has been given to the customer. An interesting aspect of this tiered system is that the government may use greater process when lesser process would satisfy the statute—for instance, the government may use a warrant when a subpoena would suffice.[33]

---

[26] *Id.* § 2702(a)(2)(A).

[27] *Id.* § 2702(a)(2)(B).

[28] *See* Juror Number One v. Superior Court, 206 Cal. App. 4th 854 (2012).

[29] *Id.* § 2702(a)(3).

[30] *See, e.g.*, Right to Financial Privacy Act, 12 U.S.C. § 3401; Video Privacy Protection Act, 18 U.S.C. § 2710; Family Educational Rights and Privacy Act of 1978, 20 U.S.C. § 1232g.

[31] *Id.* § 2702(b).

[32] *Id.* § 2702(c).

[33] Orin K. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1220 (2004).

At the highest level, Section 2703(a) requires the government to obtain a warrant if it seeks access to the *content* of a communication from an ECS provider that has been in "electronic storage" for 180 days or less.[34] Moving down a tier, if the communication has been stored for longer than 180 days, or if it is being "held or maintained" by an RCS "solely for the purpose of providing storage or computer processing services," the government can use a subpoena or a court order under Section 2703(d) so long as notice is provided to the customer at some point.[35] Section 2703(d) orders require the applicant to prove "specific and articulable facts, showing that there are reasonable grounds to believe that the contents of a[n] ... electronic communication ... are relevant and material to an ongoing criminal investigation."[36]

While Section 2703 facially permits government access to the contents of emails stored more than 180 days or those no longer in electronic storage, a 2010 ruling from the Sixth Circuit Court of Appeals calls into question the constitutional validity of this provision. In *United States v. Warshak*, the government accessed 27,000 emails directly from the suspect's Internet service provider (ISP) with a subpoena under Section 2703(b) and an ex parte order under Section 2703(d).[37] The Sixth Circuit held that such access was unlawful under the Fourth Amendment as subscribers enjoy "a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP'" and "to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional."[38]

In addition to the content of communications, the SCA permits access to non-content information with a warrant, but the government may also use a subpoena or a Section 2703(d) order without having to provide the customer notice.[39] To access basic subscriber information, including the customer's name, address, phone number, length of service, and means of payment (including bank account numbers), the government may follow the more stringent requirements for obtaining a warrant or a Section 2703(d) order, but can also use an administrative subpoena, which requires no prior authorization by a judicial officer.[40]

With forced government disclosures under Section 2703, much hinges on whether a communication is held in "electronic storage."[41] "Electronic storage" is defined as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[42] Emails that are pending delivery or have not been opened are considered to be in "temporary, immediate storage," thus,

---

[34] 18 U.S.C. § 2703(a).

[35] Section 2705, Title 18, United States Code, permits delayed customer notice under some circumstances.

[36] *Id.* § 2703(d). A §2703(d) order is similar to the *Terry* rule applied to law enforcement stop and frisks, which requires less than probable cause to believe a crime has been committed, but more than a mere hunch. Terry v. Ohio, 392 U.S. 1, 21 (1968).

[37] United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

[38] *Id.* at 288.

[39] 18 U.S.C. § 2703(c). Non-content information such as the to/from line in emails is generally not protected under the Fourth Amendment. *See* United States v. Forrester, 521 F.3d 500, 509 (9th Cir. 2007).

[40] 18 U.S.C. § 2703(c).

[41] *See* 18 U.S.C. § 2703(a) ("A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system.... ") (emphasis added).

[42] 18 U.S.C. § 2510(17).

are considered in "electronic storage."[43] Once emails are opened, however, they are no longer in "temporary, intermediate storage."[44]

Lower federal courts have taken different approaches in determining whether opened emails could be considered stored for "backup purposes" as provided in subsection (B). Some courts have held that opened emails can *never* fall within the definition of "electronic storage," as the term "backup protection" in subsection (B) was only intended to cover the protection of communications in the event the email system crashed before transmission was complete.[45] The district court in *United States v. Weaver* provided a more nuanced analysis when addressing whether opened emails left solely on a Hotmail account, a "web-based email system[]," could nonetheless be considered stored for "backup purposes."[46] The district court observed that because the emails were never downloaded by the user, but instead were solely stored on Microsoft's servers, Microsoft could not be considered as storing them for backup purposes.[47] Instead, Microsoft was "maintaining the messages 'solely for the purpose of providing storage or computer processing services to such subscriber or customer.'"

In contrast, the Ninth Circuit Court of Appeals held in *Theofel v. Farey-Jones* that emails left on a service provider's server after users downloaded them through their workplace email program could be considered stored for "backup purposes."[48] The rationale was that the email left on the server after delivery provided a "second copy" in case the customer needed to download it again. However, the court noted that "prior access" to the emails was "irrelevant," and that the appropriate inquiry is whether "the underlying message has expired in the normal course."[49] This seemingly fact-intensive inquiry has been called into question as "quite implausible and hard to square with the statutory text."[50] In any event, several of the major ECPA reform proposals would expand ECPA's reach and rely less on the definition of "electronic storage" for determining which statutory safeguards would apply.[51]

The lower federal courts have held that the SCA applies to the disclosure of various electronic communications and associated data, including

- Emails[52]

[43] Fraser v. Nationwise Mut. Ins. Co., 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001) ("It is clear that the Stored Communications Act covers a message that is stored in intermediate storage temporarily, after the message is sent by the sender, but before it is retrieved by the intended recipient."); *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 511-12 (S.D.N.Y. 2001).

[44] *See In re DoubleClick Inc.*, 154 F. Supp. 2d at 512.

[45] *Fraser*, 135 F. Supp. 2d at 636; Lazette v. Kulmatycki, 949 F. Supp. 2d 748 (N.D. Ohio 2013).

[46] United States v. Weaver, 636 F. Supp. 2d 769, 771 (C.D. Ill. 2009).

[47] *Id.* at 772.

[48] Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2003).

[49] *Theofel*, 359 F. 3d at 1076.

[50] Kerr, supra note 29, at 1217.

[51] *Compare* 18 U.S.C. § 2703 ("A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is *in electronic storage in an electronic communications system*.... "), *with* S. 356, § 3, H.R. 699, § 3, S. 512, § 3, H.R. 1174, § 3 ("A governmental entity may require the disclosure by a provider of electronic communication service or remote computing service of the contents of a wire or electronic communication *that is in electronic storage with or otherwise stored, held, or maintained* by the provider.... ").

[52] *See Theofel*, 359 F. 3d at 1077.

- Text messages[53]
- Social media private messages, wall postings, and comments[54]
- Private YouTube videos[55]
- Historical cell site location information[56]

While access to these various categories of electronic data is subject to the SCA, the protections accorded to each differs depending on how long the data has been stored; whether the communication has been accessed by the user; and whether the data is considered content or non-content. For instance, in *Quon v. Arch Wireless Operating Co., Inc.*, the Ninth Circuit held that the provider of text messaging services was operating as an ECS and that text messages stored by the company were in "electronic storage."[57] Under this reading, a warrant would be required to access text messages stored 180 days or less, and lesser process would be required if the messages were stored longer than 180 days. On the other hand, in *Viacom Intern. v. YouTube Inc.*, YouTube was considered an RCS with respect to private videos stored on its site, and therefore would be subject to the lower "specific and articulable facts" standard found in Section 2703(d).[58] To a certain extent, the various ECPA reform bills attempt to eliminate some of these distinctions and would generally require a warrant to access any electronic communications.

Finally, ECPA outlines when the government must provide notice to customers when their communications have been disclosed to the government. If the government seeks the contents of an electronic communication stored by an ECS, notice must be provided as required under Federal Rule of Criminal Procedure 41.[59] If the government seeks access to the contents of electronic communications from an RCS under a Section 2703(d) order or an administrative subpoena, prior notice must be given to the customer. Additionally, the government can seek delayed notice under 18 U.S.C. § 2705.[60]

---

[53] *See* Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 901 (9th Cir. 2008).

[54] *See* Crispin v. Christian Audigier, 717 F. Supp. 2d 965, 980, 989 (C.D. Cal. 2010).

[55] *See* Viacom Intern. Inc. v. YouTube Inc., 253 F.R.D. 256, 264 (S.D.N.Y. 2008).

[56] *See*, *e.g.*, *In re* Application of the United States of America for Historical Cell Site Data, 724 F. 3d 600 (5th Cir. 2013); United States v. Davis, No. 12-12928 (11th Cir. May 5, 2015). There is a split in the lower courts whether the SCA combined with the pen register/trap trace statute (18 U.S.C. § 3123) permits access to *prospective or real-time* cell site information without a probable cause warrant. *Compare In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747, 757 (S.D. Tex. 2005) (rejecting hybrid theory), *with In re*: Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 460 F. Supp. 2d 448, 461 (S.D.N.Y. 2006) (accepting hybrid theory). There also appears to be a split in the lower courts whether the government can access so-called "cell tower dumps" under § 2703(d). A cell tower dump request is one in which the government does not seek access to data associated with a particular cell phone number, but rather access to data associated with *all* cell activity recorded by particular cell towers. *Compare In re* Application for an Order Pursuant to 18 U.S.C. § 2703(d), 964 F. Supp. 2d 674, 678 (S.D. Tex. 2013) (rejecting access to cell tower dumps under § 2703(d), *with* In the Matter of Application for Cell Tower Records Under 18 U.S.C. § 2703(d), No. H-15-136M, 2015 WL 1022018, *4 (S.D. Tex. March 9, 2015) (permitting access to cell tower dumps for ten minute period under § 2703(d)).

[57] *See Quon*, 529 F.3d at 902, *rev'd on Fourth Amendment grounds sub nom.* Quon v. City of Ontario, 560 U.S. 746 (2010).

[58] *See Viacom Intern. Inc.*, 253 F.R.D. at 264.

[59] 18 U.S.C. § 2703(a).

[60] 18 U.S.C. § 2705.

ECPA Reform Legislation

In recent years, ECPA has faced increased criticism from both the technology and privacy communities that it has outlived its usefulness in the digital era and does not provide adequate privacy safeguards for individuals' electronic communications. In March 2010, a group of technology companies, privacy advocates, and academics urged Senator Leahy, then-chairman of the Senate Judiciary Committee, to introduce legislation to bring federal electronic communications privacy laws into the digital era.[61] In light of these and other concerns, ECPA reform has seen increased legislative attention in the past few Congresses.

In May 2011, Senator Leahy filed the Electronic Communications Privacy Act Amendments Act of 2011 (S. 1011), which would have, among other things, required law enforcement to obtain a warrant before accessing the content of any electronic communication, no matter how long it had been stored or whether it had been retrieved by the recipient.[62] The following year, Senator Leahy offered this part of his ECPA bill as an amendment to a video privacy protection bill (H.R. 2471) that was being reported out of the Senate Judiciary Committee.[63] These provisions were ultimately removed from the bill and were never enacted. Representative Yoder's Email Privacy Act (H.R. 1852), introduced in the 113th Congress and nearly identical to Senator Leahy's reform bill, obtained a majority of the Members of the House as co-sponsors (272), but was not acted on by the full House.[64] In the spring of 2013, the Senate Judiciary Committee favorably reported Senators Leahy and Lee's ECPA Amendments Act of 2013 (S. 607) to the full Senate, but it was never taken up by the full body.

The ECPA Amendments Act of 2015 (S. 356, H.R. 283)[65] and the Email Privacy Act (H.R. 699)[66] were re-introduced in the 114th Congress. Similar to the past Congress, the Email Privacy Act has obtained a majority of the Members of the House as co-sponsors (261). The Online Communication and Geolocation Protection Act, which would make similar amendments to ECPA, was introduced in the 113th (H.R. 983)[67] and 114th (H.R. 656)[68] Congresses. A competing bill, the Law Enforcement Access to Data Stored Abroad (LEADS) Act (S. 512, H.R. 1174), which covers, among other things, the extraterritorial reach of ECPA orders, was first introduced in the 113th Congress[69] and has been re-introduced in the 114th Congress.[70]

[61] S.Rept. 113-64, 2-3 (2013); *see* Digital Due Process, http://www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163.

[62] *See* S. 1011, 112th Cong. (2011).

[63] H.R. 2471, 112th Cong. (2011).

[64] H.R. 1852, 113th Cong. (2013).

[65] S. 356, 114th Cong. (2015).

[66] H.R. 699, 114th Cong. (2015).

[67] H.R. 983, 113th Cong. (2013).

[68] H.R. 656, 114th Cong. (2015).

[69] S. 2871, 114th Cong. (2014).

[70] S. 512, 114th Cong. (2015); H.R. 1174, 114th Cong. (2015).

ECPA Amendments Act of 2015 (S. 356, H.R. 283) and the Email Privacy Act (H.R. 699)

Section 2 of S. 356, H.R. 283, and H.R. 699 would amend Section 2702(a)(3) of ECPA to provide that both an ECS and an RCS would be prohibited from voluntarily disclosing to a governmental entity the content of any communication and any non-content information such as subscriber information or other communications metadata. This blanket prohibition is subject to various exceptions under existing law, including required disclosure to the government under Section 2703.[71]

Section 3 of these bills contains three major reforms to accessing the *content* of communications under ECPA. First, it would place both an ECS and RCS under the same legal requirements. Second, they would eliminate the current 180-day rule found in Section 2703(a). Again, under Section 2703(a) as currently written, emails stored for 180 days or less are subject to the warrant requirement; while emails either opened or stored for more than 180 days are subject to less stringent process.[72] These bills would eliminate this temporal requirement; thus, access to emails would require a warrant no matter how long they have been stored. Third, this section would remove the interpretive difficulty of determining whether a particular communication is in "electronic storage." Recall that federal courts have disagreed whether an opened email was being held in "electronic storage."[73] This bill expands the scope of protection to include not only messages in "electronic storage," but also those "stored, held, or maintained by the provider." This would appear to bring any opened emails under the warrant umbrella.

As under existing law, the government would be authorized to access *non-content* information, described as a "record or other information pertaining to a subscriber or customer," with a warrant, a Section 2703(d) order, consent of the subscriber, or upon a formal written request if the crime being investigated is telemarketing fraud. The government would be authorized to access basic subscriber information—such as name, address, local and long distance telephone records, and means and source of payment—with a warrant, a Section 2703(d) order, or with lesser process such as a federal or state administrative subpoena, a grand jury, a trial, or a civil discovery subpoena. The authorization to use a *civil discovery* subpoena is the only new authority that this subsection would add to current law.

These bills would also alter when notice must be provided to a customer whose communications are disclosed to the government. Under the current system, customers need not be notified when the government uses a warrant to access the content of their communications from an ECS. To require the disclosure of an email that has been opened or stored for more than 180 days, the government can use lesser process than a warrant, but must provide notice to the customer. Under the proposed legislation, the government would be required to provide the customer notice if it accesses the contents of electronic communication from either an RCS or an ECS no matter if it has been stored for more than 180 days or has been opened. If the government entity accessing the information is law enforcement, it would have 10 days to give notice; all other governmental entities would have 3 days. These bills also include a provision permitting applicants for a

[71] *See supra* notes 31-32 and accompanying text.

[72] *See* "ECPA Framework," *supra* p. 3.

[73] *Compare* Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 634 (E.D. Pa. 2001), *with* United States v. Weaver, 636 F. Supp. 2d 769, 771 (C.D. Ill. 2009).

disclosure order to request that notification be delayed. If the government entity accessing the information is law enforcement, it can request a delay of not more than 180 days; all other governmental entities can request a delay of not more than 90 days.

Online Communication and Geolocation Protection Act (H.R. 656)

Like the Email Privacy Act and the ECPA Amendments Act, the Online Communication and Geolocation Protection Act (H.R. 656) would eliminate the different legal treatment given to information held by an RCS and ECS; would eliminate the 180-day rule provided under current law; and would expand the scope from communications held in "electronic storage" to those "stored, held, or maintained by that service."[74] There are, however, differences between the other reform bills and H.R. 656. First, H.R. 656 would require that any governmental entity receiving the contents of a communication provide notice to the customer within three days of receiving such information. The Email Privacy Act and ECPA Amendments Act, on the other hand, give a law enforcement agency 10 days and any other governmental entity 3 days to provide notice. (Note that delayed notice would still be permitted under Section 2705.) Second, unlike the other reform bills, H.R. 656 would not extend access to non-content information under Section 2703(c) with a civil discovery subpoena. Third, H.R. 656 does not include a "rule of construction" that is included in the other reform bills,[75] which states that nothing in the bills should be construed to prohibit the government from seeking electronic communication records directly from a target of an investigation as opposed to a service provider.

Administrative Subpoenas

While the various ECPA reform bills discussed above appear to enjoy broad support among technology, civil liberty, and government constituencies,[76] some federal agencies have argued that passage of these bills would significantly curtail their ability to conduct investigations. In an apparent effort to assuage these concerns, the Email Privacy Act, the ECPA Amendments Act, and the LEADS Act include a "rule of construction" noting that these agencies could still seek electronic communications directly from the target of their investigation.

Currently, many federal agencies possess subpoena authority which allows them to compel the production of documents from providers without prior approval of a court.[77] Pursuant to Section

[74] H.R. 656, 114th Cong. (2015).

[75] *See infra* note 91 and accompanying text.

[76] *See*, *e.g.*, Letter to Senate Judiciary Committee from Coalition of Companies and Organizations (January 22, 2015), *available at* https://cdt.org/insight/letter-to-senate-judiciary-committee-in-support-of-ecpa-amendments-act/; BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES, EXECUTIVE OFFICE OF THE PRESIDENT 66 (2014) ("Congress should amend ECPA to ensure the standard of protection for online, digital content is consistent with that afforded in the physical world—including by removing archaic distinctions between email left unread or over a certain age."); *ECPA Part 1: Lawful Access to Stored Content: Hearing Before the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations of the H. Comm. on the Judiciary*, 113th Cong. 4 (2013) (statement of Elana Tyrangiel, Acting Assistant Attorney General, Office of Legal Policy) ("Many have noted—and we agree—that some of the lines drawn by the SCA that may have made sense in the past have failed to keep up with the development of technology, and the ways in which individuals and companies use, and increasingly rely on, electronic and stored communications. We agree, for example, that there is no principled basis to treat email less than 180 days old differently than email more than 180 days old. Similarly, it makes sense that the statute not accord lesser protection to opened emails than it gives to emails that are unopened.").

[77] *See* Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and (continued...)

2703(b), federal agencies have issued subpoenas to service providers to obtain subscriber information about individuals, including their names, telephone numbers, email addresses, and physical addresses,[78] and have indicated that they have used this authority to obtain the content of emails held by service providers for more than 180 days.[79]

Administrative subpoenas are subject to a lower evidentiary standard than the probable cause threshold required to obtain a warrant.[80] Courts reviewing such subpoenas, whether in response to a motion to quash the subpoena or at the behest of the agency seeking to enforce the subpoena in court, do so under the Fourth Amendment's general protection against unreasonableness.[81] The Supreme Court has explained that in order for such subpoenas to be upheld: (1) the investigation must be for a legitimate purpose; (2) the materials sought must be relevant to the purpose; (3) the agency must not already possess the information; and (4) the agency must have followed the proper procedural steps.[82] The Court has also indicated that information sought must be "reasonably relevant" to the investigation,[83] and "sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome."[84] The relevancy standard is a relatively low evidentiary threshold. In the grand jury context, the Court has observed that a subpoena will be quashed on relevancy grounds only when a court finds that there is "no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject" of the investigation.[85]

Generally, federal district courts have a duty to enforce proper subpoenas and may not restrict their scope unless they are "plainly incompetent or irrelevant to any lawful administrative purpose."[86] The Supreme Court has made clear that agencies are not required by the Constitution to notify the target of an investigation when subpoenaing information from third parties.[87] In response to a subpoena, a recipient may raise privileges to protect information from disclosure, such as the attorney-client and work-product privileges.[88]

All of the major ECPA reform bills would require a warrant to obtain the contents of electronic communications held by service providers, whether held for more or less than 180 days. One

(...continued)

Entities, U.S. Dep't of Justice, Office of Legal Policy, *available at* http://www.justice.gov/archive/olp/rpt_to_congress.htm.

[78] *See, e.g.*, United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010).

[79] *See* Letter from Mary Jo White, SEC Commissioner, to Senator Patrick J. Leahy, Chairman of the Senate Judiciary Committee (April 24, 2013), *available at* https://www.cdt.org/files/file/SEC%20ECPA%20Letter.pdf.

[80] *See* United States v. Powell, 379 U.S. 48, 57-58 (1964); U.S. CONST. amend. IV.

[81] *See* Oklahoma Press Pub. Co. v. Walling, 327 U.S. 186, 208 (1946) ("The gist of the protection is in the requirement, expressed in terms, that the disclosure sought shall not be unreasonable."); Doe v. United States, 253 F.3d 256, 263 (6th Cir. 2001); *In re* Subpoena Duces Tecum, 228 F.3d 341, 347 (4th Cir. 2000).

[82] *See* United States v. Powell, 379 U.S. 48, 57-58 (1964). *But see* United States v. Bell, 564 F.2d 953, 959 (Temp. Emer. Ct. App. 1977) (requiring only the first two factors in approving an administrative subpoena).

[83] U.S. v. Morton Salt, 338 U.S. 632, 652 (1950).

[84] See v. City of Seattle, 387 U.S. 541, 544 (1967).

[85] United States v. R. Enterprises, 498 U.S. 292, 301 (1992).

[86] Endicott Johnson Corp. v. Perkins, 317 U.S. 501, 509 (1943).

[87] *See* S.E.C. v. Jerry T. O'Brien, Inc., 467 U.S. 735, 741-42 (1984).

[88] *See, e.g.*, N.L.R.B. v. Interbake Foods, LLC, 637 F.3d 492, 499 (4th Cir. 2011); Director, Office of Thrift Supervision v. Vinson & Elkins, LLP, 124 F.3d 1304, 1306–07 (D.C.Cir. 1997); NLRB v. Harvey, 349 F.2d 900, 907 (4th Cir. 1965).

result of this provision would be that administrative subpoenas—subject to a lower standard of proof than warrants—would no longer be sufficient to compel service providers to produce the contents of electronic communications. However, because most federal agencies—other than the Department of Justice (DOJ)—do not possess independent authority to seek a warrant from a magistrate judge,[89] such legislation would appear to preclude agencies conducting an investigation to obtain the contents of electronic communications held by service providers directly from the provider itself. Instead, in order to do so, agencies would presumably need to rely on the DOJ to seek a warrant, whose authority is limited to doing so in criminal investigations.[90]

However, the Email Privacy Act, the ECPA Amendments Act, and the LEADS Act specify a "rule of construction" that would clarify that agencies may use subpoenas to obtain the contents of electronic communications from an "originator, addressee, or intended recipient."[91] While agencies thus could not use a subpoena to obtain the contents of electronic communications directly from service providers, they might still do so from the individuals who sent or received certain messages. In addition, the rule of construction would make clear that administrative agencies might seek the contents of electronic communications from corporations where the emails were from officers or employees of the corporation and the corporation was serving "as an electronic communications service provider for its own internal email system."[92] So, if Company X provided in-house email services to its employees, the government could seek those communications directly from the company under the SCA.

Legislation requiring a warrant to access the contents of electronic communications held by service providers appears to codify the requirements announced by the U.S. Court of Appeals for the Sixth Circuit in *U.S. v Warshak*.[93] In that case, the DOJ obtained a subpoena under Section 2703(b) compelling the target of a criminal investigation's ISP to turn over the contents of his emails to the government.[94] The Sixth Circuit held that because subscribers have a reasonable expectation of privacy in the content of email "stored with, or sent or received through, a commercial ISP," the government must obtain a warrant based on probable cause to access them.[95]

Nevertheless, at least one federal agency has claimed that the new warrant requirement contained in the reform bills would unduly restrict its investigative authority. The Securities and Exchange Commission (SEC), in a letter to the Senate Judiciary Committee, noted that the targets of agency

[89] FED. R. CRIM. P. 41.

[90] Id. Alternatively, if the agency issued a subpoena directly to an individual compelling the disclosure of the contents of electronic communications held by a service provider, a court might find that those contents were nonetheless within the individual's control and compel their production. *Cf.* Flagg v. City of Detroit, 252 F.R.D. 346, 359 (E.D. Mich. 2008) (finding that text messages held by a service provider were within the defendant's control for the purposes of Federal Rule of Procedure 34 and were subject to disclosure consistent with the SCA); Mintz v. Mark Bartelstein & Associates, Inc., 885 F. Supp. 2d 987, 994 (C.D. Cal. 2012) ("Because Plaintiff is the 'originator' of his text messages, he may request copies of these messages from AT&T consistent with the SCA. See 18 U.S.C. § 2702(b)(2).").

[91] H.R. 699, § 3, 114th Cong. (2015) ; S. 356, § 3, 114th Cong,; H.R. 283, § 3, 114th Cong. (2015); S. 512, § 3, 114th Cong. (2015); H.R. 1174, § 3, 114th Cong. (2015).

[92] S.Rept. 113-34, at 9 (2013).

[93] 631 F.3d 266, 288 (6th Cir. 2010).

[94] *Id*. at 283.

[95] *Id*. at 288 (quoting Warshak v. United States, 490 F.3d 455, 472 (6th Cir. 2007), reh'g en banc granted, opinion vacated (Oct. 9, 2007)).

investigations do not always "retain copies of their incriminating communications or may choose not to provide the e-mails in response to Commission subpoenas."[96] Accordingly, the letter argued, the SEC has historically relied on authority under Section 2703(b) to obtain the contents of electronic communications from service providers during its investigations. The legislation would foreclose the SEC from doing so in the future, thereby weakening its investigative authority. The letter argued that if the individuals under investigation knew that the SEC cannot go directly to the service providers to obtain the contents of emails, then those individuals would be less likely to be forthcoming in response to subpoenas issued directly to them. The letter concluded by suggesting that the legislation be amended by inserting a provision that would allow a federal civil agency to seek the contents of electronic communications from service providers subject to a standard similar to that governing the issuance of criminal search warrants.

However, various civil liberties groups pushed back against this position. In a letter to the SEC, a collection of privacy advocates questioned the necessity of obtaining the contents of electronic communications directly from service providers.[97] First, the letter argued that the agency had not done so since the Sixth Circuit Court of Appeals' 2010 decision in *Warshak*, and had rarely done so prior to that case. Second, the letter pointed to alternative methods of obtaining the contents of email, such as seeking to enforce a subpoena directly on the individual who is the target of an investigation in federal court. In addition, the letter argued that the authority sought by the SEC could lead to abuse. Information obtained via subpoena could be shared with the DOJ in a parallel criminal investigation, thus avoiding the warrant requirement. The attorney-client privilege could be violated in the collection of personal emails if the target of such a subpoena was not permitted to filter the emails for privileged material. The letter proposed its own amendment to potential legislation, which would clarify that administrative agencies could use subpoenas to require individuals to obtain and disclose information held by a third party.

Law Enforcement Access to Data Stored Abroad Act (LEADS Act) (S. 512, H.R. 1174).

Like the Email Privacy Act, the ECPA Amendments Act, and the Online Communication and Geolocation Privacy Act, the Law Enforcement Access to Data Stored Abroad Act (LEADS Act) would require a warrant based on probable cause to obtain the contents of communications from both an ECS and RCS and eliminate the 180-day rule.[98] In fact, the LEADS Act would provide all the other amendments to ECPA contained in both the Email Privacy Act and the ECPA Amendments Act (e.g., notice requirements, the "rule of construction," and authority to use civil discovery subpoenas for non-content information).

In addition to these changes, the LEADS Act would authorize the government to obtain the contents of electronic communications regardless of where those contents are stored if the account holder is a U.S. person.[99] This perceived need to extend ECPA's reach extraterritorially

[96] Letter from Mary Jo White, Chair of the Securities and Exchange Commission, to Senator Patrick J. Leahy, Chair of the Senate Judiciary Committee (April 24, 2013).

[97] Letter from American Civil Liberties Union, et al., to Mary Jo White, Chair of the Securities and Exchange Commission (April 9, 2014), *available at* https://d1ovv0c9tw0h0c.cloudfront.net/files/2014/04/SEC-ECPA-reform.pdf.

[98] *See* Law Enforcement Access to Data Stored Abroad Act, H.R. 1174, 114th Cong. (2015); Law Enforcement Access to Data Stored Abroad Act, S. 512, 114th Cong. (2015).

[99] *Id*. at § 3.

has been prompted, in part, by two facets of the Internet. The first is the fact that service providers can store customer data in fragmented form in multiple locations including overseas.[100] The second is that data is not always stored in the same country as the user.[101]

The LEADS Act would partially address an issue currently being litigated in federal court—whether, under ECPA, the government can compel third-party service providers to produce the contents of electronic communications held overseas. In a pending case in the U.S. Court of Appeals for the Second Circuit, the United States sought and received a warrant from a federal magistrate judge under Section 2703(a) of ECPA for the contents of emails and subscriber information for an email account operated by Microsoft Corporation.[102] Microsoft complied with the portion of the warrant seeking non-content information, which was stored on servers located inside the United States. However, Microsoft determined that the content information sought by the warrant was located in servers hosted in Dublin, Ireland and moved to quash that aspect of the warrant.

In its challenge, Microsoft argued that because federal courts generally lack authority to issue warrants for the search and seizure of items located outside of the United States, the warrant issued here was therefore unauthorized.[103] The magistrate judge—and, subsequently, the district court judge—rejected this argument and upheld the warrant.[104] The court reasoned that Section 2703(a) warrants were not traditional warrants but hybrids, with aspects similar to both subpoenas and traditional warrants. In contrast to traditional warrants, subpoenas require the disclosure of information within a recipient's control, regardless of location (even if overseas). In addition, when executing Section 2703(a) warrants, government officials do not view any information until it arrives in the United States, so no extraterritorial search occurs

While resolution of this question, at least in the Second Circuit, awaits the court's decision, the LEADS Act would at least partially clarify the government's authority in this area. The act would require third-party service providers to disclose the contents of U.S. persons' electronic communications held overseas upon issuance of a warrant based on probable cause.[105] However, the legislation contains an exception: courts issuing such warrants shall modify or vacate the warrant if, upon a motion by the service provider, the court finds that disclosure would force the service provider to violate the laws of a foreign country.[106] Given the variety of legal privacy regimes in other countries and the relative ease with which major service providers can relocate and store data around the world, it is unclear precisely how these provisions of the LEADS Act would affect email privacy.

In addition, while the bill specifically would authorize the government to compel the disclosure of the contents of communications held by third-party service providers overseas if the account

[100] *See* Kerr, *supra* note 17, at 408.

[101] *See In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 469 (S.D.N.Y. 2014).

[102] *Id.* at 477.

[103] *Id*. at 470.

[104] *Id*. at 477; *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., No. 13-MJ-2814, 2014 WL 4629624, at *1 (S.D.N.Y. Aug. 29, 2014) ("On July 31, 2014, the Court heard oral argument on those objections and affirmed Judge Francis's ruling by issuing the July 31 Order on the record.").

[105] Law Enforcement Access to Data Stored Abroad Act, S. 512, 114th Cong. § 3(a)(2) (2015).

[106] *Id*.

holder is a U.S. person, it is silent as to non-U.S. persons.[107] Were the LEADS Act to become law, this omission would raise the question whether the government would be barred from issuing a warrant or a subpoena to require a service provider to disclose the contents of communications of non-U.S. persons held overseas. For example, assuming law enforcement was investigating criminal activity involving a U.S. person in concert with a non-U.S. person visiting the United States—would the government be permitted to compel the disclosure of the emails held overseas of the U.S. person, but not the non-U.S. person?

One interpretation of this omission is that the broad privacy protections contained in Section 2702 would bar providers from disclosing the contents of communications of non-U.S. persons held overseas, and because Section 2703, under existing law or as amended by the LEADS act, does not specifically authorize the government to obtain a warrant compelling a service provider that stores information overseas to disclose them, the government is precluded under Section 2702 from obtaining them. Relying on the canon of statutory interpretation *expressio unius est exclusio alterius* ("expressing one item of an associated group or series excludes another left unmentioned"),[108] it might be argued that the LEADS Act's express inclusion of U.S. persons could be interpreted to mean that the communications of non-U.S. persons were not intended to fall within the reach of this new rule.

However, an alternative view would be that while the LEADS Act appears to lack any *authorization* for the government to obtain a warrant to compel the disclosure of the contents of communications of non-U.S. persons held overseas, the privacy protections of Section 2702 are simply inapplicable to such contents and do not bar the government from seeking them by other means. The "presumption against extraterritorial application" of U.S. law teaches that if a statute "gives no clear indication of an extraterritorial application, it has none."[109] And even "when a statute provides for some extraterritorial application, the presumption ... operates to limit that provision to its terms."[110] If one considers an ECPA warrant compelling a service provider to disclose the contents of communications held overseas to authorize a law enforcement seizure abroad, rather than simply directing an entity to act within the United States—a question currently under litigation in the Second Circuit Court of Appeals[111]—then the presumption against extraterritorial application of U.S. law would presumably apply. In that case, the statute must clearly indicate that the privacy protections of Section 2702 apply abroad. Failing that, the relevant provisions of Section 2702 would not protect the contents of communications of non-U.S. persons held abroad, and the government could conceivably rely on alternative authorities to compel disclosure, such as a traditional subpoena.[112] This issue, as well as other interpretive questions raised by ECPA reform, would likely have to be resolved through litigation.

---

[107] *Id*.

[108] Chevron U.S.A. Inc. v. Echazabal, 536 U.S. 73 (2002) (quoting United States v. Vonn, 535 U.S. 55, 65 (2002)).

[109] Morrison v. National Australia Bank Ltd., 561 U.S. 247, 255 (2010). However, another rule of construction, derived from *United States v. Bowman*, 260 U.S. 94 (1922), teaches that Congress "need not expressly provide for extraterritorial application of a criminal statute if the nature of the offense is such that it may be inferred." United States v. MacAllister, 160 F.3d 1304, 1307-08 (11th Cir. 1998).

[110] *Id*. at 265.

[111] *See* Brief for Appellant, In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp. (2d Cir. Dec. 8, 2014).

[112] Whether a traditional subpoena could be used to compel service providers to disclose the contents of emails of non-U.S. persons held by the provider overseas is beyond the scope of this report. *See generally* United States v. Verdugo-Urquidez, 494 U.S. 259, 274-75 (1990) (holding that Fourth Amendment does not apply to searches of non-U.S. persons outside of the United States).

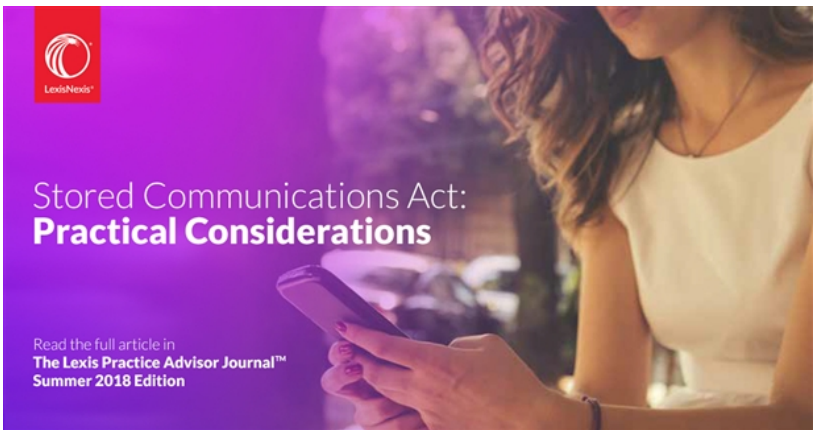
Author Contact Information

Richard M. Thompson II
Legislative Attorney
rthompson@crs.loc.gov, 7-8449

Jared P. Cole
Legislative Attorney
jpcole@crs.loc.gov, 7-6350

Stored Communications Act: Practical Considerations

Posted on 06-22-2018



(/lexis-practice-advisor/cfs-file.ashx/__key/communityserver-blogs-components-weblogfiles/00-00-00-00-03/183994_2D00_M_2D00_LPA_2D00_Journal_2D002800_Summer_2D00_Edition_29002D00_Article_2D00_Images_2D00_storedcommunication_2E00__2E00__2E00_.jpg)

By: **Michael E. Lackey** and **Oral D. Pottinger**, Myer Brown LLP

The Stored Communications Act (SCA), 18 U.S.C. § 2701 et seq., governs the disclosure of electronic communications stored with technology providers. Passed in 1986 as part of the Electronic Communications Privacy Act (ECPA), the SCA remains relevant to address issues regarding the privacy and disclosure of emails and other electronic communications.

AS THE USE OF TECHNOLOGY CONTINUES TO GROW, SO does the importance of the SCA's protections–and limits–on the disclosure of stored electronic communications. The SCA's age, however, makes it difficult to apply in modern times. This article provides guidance on how to apply the SCA to today's fast-growing technology.

Understanding How SCA Issues Arise

As a privacy statute, diverse circumstances can give rise to SCA issues:

- **Direct liability.** As discussed below, the SCA limits the ability of certain technology providers to disclose information. It also limits third parties' ability to access electronic communications without sufficient authorization. Litigation alleging violations of the SCA's substantive provisions therefore directly presents SCA issues
- **Civil subpoena limitations.** Because of the SCA's restrictions on disclosure, technology providers and litigants often invoke the SCA when seeking to quash civil subpoenas to technology providers for electronic communications.[1]
- **Government investigations.** The SCA provides a detailed framework governing law enforcement requests for electronic communications. SCA issues often arise in motions to suppress and related criminal litigation. For example, a growing number of courts have found that the SCA is unconstitutional to the

> extent that it allows the government to obtain emails from an internet service provider without a warrant in violation of the Fourth Amendment. See U.S. v. Warshak, 631 F.3d 266 (6th Cir. 2010).

Additionally, the circuit conflict about whether technology providers and litigants can invoke the SCA when quashing criminal subpoenas or search warrants requesting data from extraterritorial servers, was resolved by the passage of the CLOUD Act as part of the Consolidated Appropriations Act, 2018, H.R. 1625, Div. V, 115th Cong., 2d Sess. (2018). The Act provides that a service provider must produce information within its "possession, custody, or control, regardless of whether such . . . information is located within or outside of the United States." CLOUD Act § 103(a). The passage of the CLOUD Act also rendered moot the U.S. v. Microsoft case pending before the Supreme Court on this issue. See U.S. v. Microsoft Corp., No. 17-2, slip op. at 3 (April 17, 2018) (dismissing the appeal as moot). The government has subsequently obtained a new warrant against Microsoft for the information requested in the original warrant at issue in the case.

Categorizing the Technology Involved in an SCA Claim

The technology behind an SCA claim matters. In many instances, the applicable SCA rules hinge on the particular technology involved. Specifically, different SCA rules apply depending on whether technology is classified as electronic communication services (ECS), remote computing services (RCS), both, or neither.

The following sections discuss the definitions of ECS and RCS, the rules applicable to each, and certain applications of these definitions. While you should familiarize yourself with these concepts, you must exercise caution in applying them. Courts have reached disparate results, and this area continually evolves with each new technological development.

Electronic Communication Services

The SCA defines an ECS as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[2] With certain exceptions, ECS providers may not "knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service."[3]

Clear examples of an ECS include an email provider's computer systems, a bulletin board system, or an internet service provider (ISP).[4] In addition, courts have classified text message service providers as ECS providers.[5] Even if providing a messaging service or internet service is not the entity's primary business, the entity can qualify as an ECS provider.[6]

As a practical matter, the definition of ECS often plays an important role in e-discovery matters. Because the SCA prohibits ECS providers from disclosing the contents of communications stored with them, do not expect to succeed in obtaining these communications by subpoenaing an ECS provider, such as a social media website or email vendor. Instead, you should request these records from the creator or recipient of such content.

Remote Computing Services

In contrast, the SCA defines an RCS as providing to the public "computer storage or processing services by means of an electronic communications system."[7] Again with certain exceptions, the SCA prohibits RCS providers from knowingly divulging to any person or entity the contents of any communication that the service carries or maintains:

- On behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service
- Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing[8]

For example, a U.S. District Court in Illinois found that Microsoft's Hotmail's email service was an RCS because it found that "Microsoft [was] maintaining the messages 'solely for the purpose of providing storage or computer processing services to such subscriber or customer.'"[9]

Both ECS and RCS

In some instances, courts have concluded that modern technology providers act as both ECS and RCS providers with the different services they offer.[10] In Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010), the court concluded that social media websites were ECS providers, but alternatively held that they were RCS providers.

Where a provider acts as both an ECS and RCS, the SCA's applicable rules will apply to those aspects of the service that fit within the respective definitions.

Neither ECS nor RCS

In some instances, neither an ECS nor an RCS provider holds electronic communications. "[A] person who does not provide an electronic communication service [or a remote communication service] can disclose or use with impunity the contents of an electronic communication unlawfully obtained from electronic storage."[11]

In general, courts have concluded that personal devices, such as laptop computers and smartphones, do not provide electronic communications services for purposes of the SCA, even though they allow users to access such services.[12] Thus, individual computer users generally do not count as ECS or RCS providers.

However, while the SCA's disclosure limits would not apply, even entities that do not qualify as ECS or RCS providers can fall afoul of the SCA's limits on unauthorized access.[13] Importantly, the SCA provides for criminal and civil penalties for anyone who:

- Intentionally and without sufficient authorization
- Accesses "a facility through which an electronic communication service is provided"
- And in doing so, "obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system"[14]

Because the SCA does not prohibit the disclosure of information by non-ECS or RCS providers, you should not rely on it to protect against all possible disclosures of sensitive electronic communications.[15] Instead, you should counsel employers to maintain close control over individual devices, such as company laptops and cell phones.

Determining What Is in Electronic Storage

The SCA's ECS restrictions, 18 U.S.C. § 2702(a)(1), and access restrictions, 18 U.S.C. § 2701, only apply to communications that are in electronic storage. Electronic storage means:

- Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof
- Any storage of such communication by an ECS for purposes of backup protection of such communication[16]

In today's world of cloud computing and remote hosting, applying this definition can prove difficult. In particular, courts continue to struggle with whether documents stored remotely, such as web-based email, are stored "for purposes of backup protection" or for some other purpose that would render them outside the scope of the SCA's definition.[17] Nonetheless, certain general principles can help you analyze this portion of a potential SCA claim:

- Messages (such as emails, bulletin board postings, or pager messages) being stored pending delivery are generally deemed to be in electronic storage for purposes of the SCA.[18]
- Items stored on personal devices, such as cookies (small pieces of data stored on an internet user's computer) and text messages are generally not deemed to be in electronic storage for purposes of the SCA.[19]
- Messages that have already been delivered and read, but that a user chooses to leave on the server, have produced divergent results. Courts disagree on whether such emails are stored "for purposes of backup protection."[20]

Because technology continues to change, and in light of the disagreement among the courts in applying the SCA's definitions to today's technology, you should exercise caution in coming to fixed conclusions about the SCA's implications to particular facts.

Analyzing "Authorization"

Proper analysis of an SCA claim under 18 U.S.C. § 2701 also requires you to examine the factual question of whether the defendant acted "without authorization" or "exceed[ed] an authorization" in accessing the facility involved. In general, "[p]ermission to access a stored communication does not constitute valid authorization if it would not defeat a trespass claim in analogous circumstances."[21]

However, where an individual was "entitled to see" the information, courts do not generally find liability.[22] This result holds even where an individual puts the electronic communications to unauthorized use.[23] Relatedly, joint use of a computer will often preclude an SCA claim by one user against another.[24]

This issue often arises in the context of post-termination employment disputes. Terminated employees may retain access credentials or otherwise seek to obtain electronic records from the company. While the SCA may provide an employer with a remedy against such actions, a successful claim usually necessitates clear evidence that the employer had revoked the employee's authorization before the employee accessed the information.[25] You should therefore counsel clients to develop policies that will facilitate such proof.

Exceptions to SCA Prohibitions

The SCA includes many exceptions to its prohibitions, which the following sections discuss.

Certain Authorized Conduct

The SCA[26] does not apply with respect to conduct authorized:

- By the person or entity providing a wire or electronic communications service
- By a user of that service with respect to a communication of or intended for that user
- In Section 2703 (government access, 18 U.S.C. § 2703), 2704 (backup preservation, 18 U.S.C. § 2704), or 2518 (courtordered electronic eavesdropping or wiretaps, 18 U.S.C. § 2518)

Allowable Disclosures of Communication Contents

The SCA allows providers of an RCS or ECS to disclose the contents of a communication:

- To an addressee or intended recipient of such communication or an agent of such addressee or intended recipient
- As otherwise authorized in Sections 2517, 2511(2)(a), or 2703 of the SCA
- With the lawful consent of the originator or an addressee or intended recipient of such communication or the subscriber in the case of an RCS
- To a person employed or authorized or whose facilities are used to forward such communication to its destination
- As may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service
- To the National Center for Missing and Exploited Children, in connection with a report submitted thereto under Section 2258A
- To a law enforcement agency if the contents (1) were inadvertently obtained by the service provider and (2) appear to pertain to the commission of a crime
- To a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency[27]

Consent Exception

The consent exception (18 U.S.C. § 2702(b)(3)) is one of the more common exceptions to arise under the SCA. In addition to allowing disclosures with the sender's consent, this exception also allows the disclosure of communications directed to the service provider.[28]

Allowable Disclosures of Information Concerning a Subscriber or Customer

The SCA allows providers of an RCS or ECS to disclose information concerning a subscriber to, or customer of, such service (not including contents of communications covered by 18 U.S.C. § 2702 (a)(1) or (a)(2)):

- As otherwise authorized in 18 U.S.C. § 2703
- With the lawful consent of the customer or subscriber
- As may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service
- To a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency
- To the National Center for Missing and Exploited Children, in connection with a report submitted thereto under 18 U.S.C. § 2258A
- To any person other than a governmental entity[29]

Court Orders, Warrants, Subpoenas, Statutory Authorization, or Certifications

The SCA has an exception for ECS providers who provide information in response to a legal mandate. Specifically:

> No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.[30]

Through this exception, service providers can disclose information not only in response to court orders and law enforcement requests, but also in cases of crisis. Specifically "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency."[31]

Good Faith Defense

The SCA allows a complete defense when a defendant can show good faith reliance on:

- A court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under Section 2703(f))
- A request of an investigative or law enforcement officer under 18 U.S.C. § 2518 (7)
- A good faith determination that 18 U.S.C. § 2511(3) permitted the complained-of conduct[32]

If a recipient of an SCA request complies with the request in good faith, it will enjoy immunity from suit even if the request is later determined to be invalid.[33] While courts differ slightly in their tests for determining whether a recipient has acted in good faith, the question generally boils down to reasonableness.[34] This exception lowers the burden on recipients to scrutinize requests under the SCA for all potential flaws.

Statutory, Actual, and Punitive Damages

With respect to direct liability, you should take note that a plaintiff suing under 18 U.S.C. § 2707 for violations of the SCA can pursue either (1) their actual damages and any profits the violator obtained or (2) $1,000. The statute also provides for punitive damages.

Courts disagree, however, about whether a plaintiff must show some amount of actual damages in order to trigger the statutory damages provision.[35] Thus, you should take careful note of the jurisdiction in which an SCA claim is brought, as this disagreement may have significant implications for how a case is litigated. But note that even *Van Alstyne* holds that punitive damages may be available in the absence of proof of actual damages.

Secondary Liability

Courts generally agree that, although the SCA creates civil liability for violations of its prohibitions, it does not create secondary civil liability, such as for aiding and abetting or conspiracy.[36]

Other Potentially Relevant Law

The SCA is not the only statute governing the disclosure of electronic communications. Many cases involving electronic communications also involve potential liability under the Wiretap Act, 18 U.S.C. § 2510 et seq., which was also passed as part of the Electronic Communication Privacy Act. In addition, depending on the facts involved, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, the Pen Register Act, 18 U.S.C. § 3121 et seq., or the Cybersecurity Act of 2015, 6 U.S.C. § 1501 et seq., may apply, as well as traditional common-law doctrines such as trespass and intrusion upon seclusion.

Michael E. Lackey leads Mayer Brown LLP's global litigation and dispute resolution practice, serves on the firm's Partnership Board, and is a co-leader of its Electronic Discovery & Information Governance group. His practice focuses on civil and criminal litigation, and he represents major companies and individuals in state and federal proceedings, including multi-district and class action litigation. In addition to being an accomplished litigator, Mike is nationally recognized for his knowledge of electronic discovery issues. Oral D. Pottinger is a senior associate in the Antitrust practice at Mayer Brown. He specializes in mergers and acquisitions, civil and criminal antitrust investigations, antitrust counseling, and Federal Communications Commission cable and media representation. Oral has served as a trusted advisor addressing the needs of corporate clients from information risk management and dataretention planning to discovery planning, e-discovery collection, data analytics, managed electronic review, and production. Special acknowledgment is provided to Sasha Keck, Mayer Brown associate, for her research assistance.

To find this article in Lexis Practice Advisor, follow this research path:

RESEARCH PATH: Labor & Employment > Employment Policies > Company Property and Electronic Information > Practice Notes (https://advance.lexis.com/open/document/lpadocument/?pdmfid=1000522&crid=8658d013-f926-4879-a5f1-e31c842953e0&pddocfullpath=%2Fshared%2Fdocument%2Fanalytical-materials%2Furn%3AcontentItem%3A5DC1-XPM1-JSRM-64V6-00000-00&pddocid=urn%3AcontentItem%3A5DC1-XPM1-JSRM-64V6-00000-00&pdcontentcomponentid=126170&pdteaserkey=sr2&pditab=allpods&ecomp=-vtg&earg=sr2&prid=bc3712dc-f0b1-45ae-a0af-455c93c956b0)

Related Content

For guidance on how to counsel employers to manage the risks that accompany employee social m

> SOCIAL MEDIA ISSUES IN EMPLOYMENT: COUNSELING EMPLOYERS ON KEY SOCI (https://advance.lexis.com/open/document/lpadocument/?pdmfid=1000522&crid=d45f 0e1555337215&pddocfullpath=%2Fshared%2Fdocument%2Fanalytical-materials%2Fu 3A5FPY-GFP1-DYV0-G0K8-00000-00&pddocid=urn%3AcontentItem%3A5FPY-GFP1- 00&pdcontentcomponentid=126170&pdteaserkey=sr0&pditab=allpods&ecomp=-vtg&e f0b1-45ae-a0af-455c93c956b0)

RESEARCH PATH: Labor & Employment > Employment Policies > Company Property and Practice Notes (https://advance.lexis.com/api/permalink/793081bb-ece0-40c8-9fd2-6fb context=1000522)

For a discussion on the key issues involving the Electronic Communications Privacy Act, see

> ELECTRONIC COMMUNICATIONS PRIVACY ACT: KEY ISSUES (https://advance.lexis.com/open/document/lpadocument/?pdmfid=1000522&crid=bbde dddcc83e2e1b&pddocfullpath=%2Fshared%2Fdocument%2Fanalytical-materials%2Fur 3A5DC1-XPM1-JSRM-64V7-00000-00&pddocid=urn%3AcontentItem%3A5DC1-XPM 00&pdcontentcomponentid=126170&pdteaserkey=sr0&pditab=allpods&ecomp=-vtg&e 295a-4734-b9dc-956f06a64d12)

RESEARCH PATH: Labor & Employment > Employment Policies > Company Property anc Practice Notes (https://advance.lexis.com/api/permalink/793081bb-ece0-40c8-9fd2-6fb context=1000522)

For additional information on the Electronic Communications Privacy Act, see

> ELECTRONIC COMMUNICATION PRIVACY ACT ISSUES CHECKLIST (https://advance.lexis.com/open/document/lpadocument/?pdmfid=1000522&crid=e47a 8ad91d575325&pddocfullpath=%2Fshared%2Fdocument%2Fforms%2Furn%3Aconten F016-S1CV-00000-00&pddocid=urn%3AcontentItem%3A5D4R-5JW1-F016-S1CV-00(00&pdcontentcomponentid=126172&pdteaserkey=sr1&pditab=allpods&ecomp=-vtg&e 0ee1-461a-b892-89da98ca4ee0)

RESEARCH PATH: Labor & Employment > Employment Policies > Company Property anc Checklists (https://advance.lexis.com/api/permalink/b49c5885-503c-4fea-9792-a22d3c context=1000522)

For guidance on how to counsel employers to manage the risks that accompany employee social m

> SOCIAL MEDIA ISSUES IN EMPLOYMENT: COUNSELING EMPLOYERS ON KEY SOCI (https://advance.lexis.com/open/document/lpadocument/?pdmfid=1000522&crid=a8e2 d72e05884360&pddocfullpath=%2Fshared%2Fdocument%2Fanalytical-materials%2Fu 3A5FPY-GFP1-DYV0-G0K8-00000-00&pddocid=urn%3AcontentItem%3A5FPY-GFP1- 00&pdcontentcomponentid=126170&pdteaserkey=sr0&pditab=allpods&ecomp=-vtg&e 3438-4ece-9027-eab17c0ef69b)

RESEARCH PATH: Labor & Employment > Employment Policies > Company Property anc Practice Notes (https://advance.lexis.com/api/permalink/793081bb-ece0-40c8-9fd2-6fb context=1000522)

For a discussion on the key issues involving the Electronic Communications Privacy Act, see

> ELECTRONIC COMMUNICATIONS PRIVACY ACT: KEY ISSUES (https://advance.lexis.com/open/document/lpadocument/?pdmfid=1000522&crid=4209 827988244292&pddocfullpath=%2Fshared%2Fdocument%2Fanalytical-materials%2Fu 3A5DC1-XPM1-JSRM-64V7-00000-00&pddocid=urn%3AcontentItem%3A5DC1-XPM 00&pdcontentcomponentid=126170&pdteaserkey=sr0&pditab=allpods&ecomp=-vtg&e 38b2-45e2-8038-24aafec8ff28)

RESEARCH PATH: Labor & Employment > Employment Policies > Company Property anc Practice Notes (https://advance.lexis.com/api/permalink/793081bb-ece0-40c8-9fd2-6fb context=1000522)

For guidance on protecting confidential information, see

> CYBERSECURITY MEASURES TO PROTECT EMPLOYERS' CONFIDENTIAL INFORM/
SECRETS (https://advance.lexis.com/open/document/lpadocument/?pdmfid=1000522&
4f1d-b082-349955830bd1&pddocfullpath=%2Fshared%2Fdocument%2Fanalytical-ma
3AcontentItem%3A5NFV-YF51-JK4W-M1Y3-00000-00&pddocid=urn%3AcontentItem
M1Y3-00000-
00&pdcontentcomponentid=126170&pdteaserkey=sr0&pditab=allpods&ecomp=-vtg&
8129-4382-a6c2-06ab893e2c81)

RESEARCH PATH: Labor & Employment > Non-competes and Trade Secret Protection > Practice Notes

1. *See* Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 264 (S.D.N.Y. 2008) (https://advance.lexis.com/api/permalink/809ccc59-19fe-432e-9597-1ffbec87eeb0/?context=1000522) (quashing subpoena), aff'd in part on other grounds, vacated in part on other grounds, 676 F.3d 19 (2d Cir. 2012) (https://advance.lexis.com/api/permalink/4e18de01-394a-4bf0-9dd4-2da367748fbd/?context=1000522); In re Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 611 (E.D. Va. 2008) (https://advance.lexis.com/api/permalink/a6ea9fb5-8646-4c64-aba4-3741022b6e59/?context=1000522); O'Grady v. Superior Court, 139 Cal. App. 4th 1423, 44 Cal. Rptr. 3d 72 (2006) (https://advance.lexis.com/api/permalink/9e302894-75ad-4faf-b6b5-9d8338ee00a8/?context=1000522). **2**. 18 U.S.C. § 2510(15) (https://advance.lexis.com/api/permalink/3adcf86c-3924-4ea7-8539-8266c1a1e3ce/?context=1000516). **3**. 18 U.S.C. § 2702(a)(1) (https://advance.lexis.com/api/permalink/a1b33d3a-7a10-4b4b-a171-d6e82de8c79b/?context=1000522). **4**. *See* In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1057 (N.D. Cal. 2012) (https://advance.lexis.com/api/permalink/3db1b4cd-89a6-4067-a057-8cbb7c0245a4/?context=1000522). **5**. *See* Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892 (9th Cir. 2008) (https://advance.lexis.com/api/permalink/1c032a34-fb29-4f2a-b648-4fe3e32d4555/?context=1000522), rev'd on other grounds, City of Ontario v. Quon, 560 U.S. 746 (2010) (https://advance.lexis.com/api/permalink/98b42ef2-642d-40ec-bf09-3d44b3546f26/?context=1000522). Courts have ruled as well for social media sites. *See* Ehling v. Monmouth-Ocean Hosp. Service Corp., 961 F. Supp. 2d 659 (D.N.J. 2013) (https://advance.lexis.com/api/permalink/758581a3-3b9c-423a-a468-bb061681edef/?context=1000522); Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010) (https://advance.lexis.com/api/permalink/4516987a-9f48-49ab-8137-1c9ff2597337/?context=1000522). **6**. *See* In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2705(b), 2018 U.S. Dist. LEXIS 19556 (D.D.C. Jan. 30, 2018) (https://advance.lexis.com/api/permalink/4410a4c3-4140-40ce-a918-790365b6b39a/?context=1000516) (Airbnb was an ECS provider as it provided a messaging service for its users to communicate with each other); In re United States for an Order Pursuant to 18 U.S.C. § 2703(d), 2018 U.S. Dist. LEXIS 52183 (D.D.C. Mar. 8, 2018) (https://advance.lexis.com/api/permalink/fd2c7ed5-1a27-4be9-8058-ac5489bbd899/?context=1000516) (Royal Caribbean Cruises provided internet service to its customers and thus qualified as an ECS provider). **7**. 18 U.S.C. § 2711(2) (https://advance.lexis.com/api/permalink/79d67fe0-6a5c-4cfd-9609-9917db1420a1/?context=1000522). **8**. 18 U.S.C. § 2702(a)(2) (https://advance.lexis.com/api/permalink/0243a35b-2026-45f3-ae4f-dc4bd3b143bd/?context=1000522). **9**. United States v. Weaver, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009) (https://advance.lexis.com/api/permalink/7e4d3f64-f026-49b4-8f13-181ae32512c9/?context=1000522) (quoting 18 U.S.C. § 2703(b)(2) (https://advance.lexis.com/api/permalink/ac41cb80-c426-4187-9c93-608d4bed8b9a/?context=1000522)). **10**. *See* United States v. Weaver, 636 F. Supp. 2d 769, 770 (C.D. Ill. 2009) (https://advance.lexis.com/api/permalink/3f417c0d-1f37-45a0-9d99-1e9dcfa76bb6/?context=1000522) (email service provider was both ECS and RCS provider); *see also* In re United

States, 665 F. Supp. 2d 1210, 1214 (D. Or. 2009) (https://advance.lexis.com/api/permalink/2e48128a-0318-4f5b-ac83-a96fdd3a00fc/?context=1000522) ("Today, most ISPs provide both ECS and RCS."). **11**. Wesley College v. Pitts, 974 F. Supp. 375, 389 (D. Del. 1997) (https://advance.lexis.com/api/permalink/007160a6-1c87-47a1-b371-724068b75f72/?context=1000522). **12**. *See* Garcia v. City of Laredo, 702 F.3d 788 (5th Cir. 2012) (https://advance.lexis.com/api/permalink/fe5b49d7-c156-47d4-be2b-df5a240b5bd0/?context=1000522); United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003) (https://advance.lexis.com/api/permalink/1175b6ec-b2ab-423a-9171-ac5c450fbbc9/?context=1000522); In re iPhone Application Litig., 844 F. Supp. 2d at 1057–58 (https://advance.lexis.com/api/permalink/3db1b4cd-89a6-4067-a057-8cbb7c0245a4/?context=1000522); In re DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001) (https://advance.lexis.com/api/permalink/ba3ae586-34b9-41da-aac7-03a5da9558ee/?context=1000522); Crowley v. CyberSource Corp., 166 F. Supp. 2d 1263, 1270–71 (N.D. Cal. 2001) (https://advance.lexis.com/api/permalink/c39f8ff0-ca73-403f-b006-c9deceb788ec/?context=1000522). **13**. *See* Penrose Computer Marketgroup, Inc. v. Camin, 682 F. Supp. 2d 202, 211 (N.D.N.Y. 2010) (https://advance.lexis.com/api/permalink/f4659a77-fd9b-484c-bd2d-79afae397fdf/?context=1000522) ("[S]ection 2701 outlaws illegal entry, not larceny.") **14**. 18 U.S.C. § 2701 (https://advance.lexis.com/api/permalink/96555f1c-dffc-4add-832b-7b92cd5912be/?context=1000522). **15**. *See K.F. Jacobsen & Co. v. Gaylor, 947 F. Supp. 2d 1120 (D. Or. 2013) (https://advance.lexis.com/api/permalink/8090904b-e654-4aa5-ba2f-407322961ce7/?context=1000522) (rejecting SCA claim because employers' individual computers were not ECS facilities). **16**. 18 U.S.C. § 2510 (17) (https://advance.lexis.com/api/permalink/3adcf86c-3924-4ea7-8539-8266c1a1e3ce/?context=1000516). **17**. See Lazette v. Kulmatycki, 949 F.Supp.2d 748, 758-59 (N.D. Ohio 2013) (discussing the divergence in opinions) (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522). **18**. See Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2003) (https://advance.lexis.com/api/permalink/458c8272-fe90-4ded-9a18-55843c92ec04/?context=1000522) (collecting cases); (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522)Quon, 529 F.3d 892. **19**. See (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522)In re DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 511 –12 (https://advance.lexis.com/api/permalink/fe5b49d7-c156-47d4-be2b-df5a240b5bd0/?context=1000522); (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522)Garcia, 702 F.3d 788. **20**. Compare (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522)Theofel, 359 F.3d 1076-77 (https://advance.lexis.com/api/permalink/458c8272-fe90-4ded-9a18-55843c92ec04/?context=1000522), (holding delivered messages were in electronic storage for purposes of the SCA); (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522) Bailey v. Bailey, 2008 U.S. Dist. LEXIS 8565, at *16–18 (E.D. Mich. Feb. 6, 2008) (https://advance.lexis.com/api/permalink/5274f5d8-6b0c-43ab-87f8-c4d7080788a8/?context=1000522) (same); (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522)Ehling v. Monmouth-Ocean Hosp. Service Corp., 961 F. Supp. 2d 667 (https://advance.lexis.com/api/permalink/758581a3-3b9c-423a-a468-bb061681edef/?context=1000522) (D.N.J. 2013) (holding that Facebook wall postings were in electronic storage) with (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522) United States v. Weaver, 636 F. Supp. 2d 771–73 (https://advance.lexis.com/api/permalink/7e4d3f64-f026-49b4-8f13-181ae32512c9/?context=1000522)(C.D. Ill. 2009) (https://advance.lexis.com/api/document?collection=cases&id=urn:contentItem:4WSH-9GD0-TXFP-T3CY-00000-00&context=) (holding previously opened messages not in electronic storage for purposes of the SCA); (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522) Jennings v. Jennings, 736 S.E.2d 242, 245 (S.C. 2012) (https://advance.lexis.com/api/permalink/eefb31f4-689a-45de-837e-57a2fa77c894/?context=1000522). **21**. (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522)

Theofel v. Farey-Jones, 359 F.3d 1073 (https://advance.lexis.com/api/permalink/458c8272-fe90-4ded-9a18-55843c92ec04/?context=1000522). ***22****. See (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522)Int'l Ass'n of Machinists & Aero. Workers v. Werner –Masuda, 390 F. Supp. 2d 479, 495 (D. Md. 2005) (https://advance.lexis.com/api/permalink/7602da2a-e53a-40a7-9834-048eab3607ce/?context=1000522).* ***23****. See (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522) Educational Testing Serv. v. Stanley H. Kaplan Educ. Ctr., 965 F. Supp. 731, 740 (D. Md. 1997) (https://advance.lexis.com/api/permalink/9d14627b-ea1b-460f-a6b5-a905c0fa36d0/?context=1000522).* ***24****. See (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522)White v. White, 781 A.2d 85, 90–91 (N.J. 2001) (https://advance.lexis.com/api/permalink/a9abc473-c724-4de4-8858-618186400270/?context=1000522); (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522)State v. Poling, 938 N.E.2d 1118, 1123 (Ohio 2010) (https://advance.lexis.com/api/document?collection=cases&id=urn:contentItem:51Y0-4931-652N-S008-00000-00&context=).* ***25****. See (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522)Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F. Supp. 2d 817, 821 (E.D. Mich. 2000) (https://advance.lexis.com/api/permalink/09f68fe2-143e-47e5-a6b2-faf32bb4fe11/?context=1000522) (rejecting SCA claim because individuals had authorization at the time of access); (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522)Lasco Foods, Inc. v. Hall & Shaw Sales, Mktg., & Consulting, LLC, 600 F. Supp. 2d 1045, 1050 (E.D. Mo. 2009) (https://advance.lexis.com/api/permalink/81b1b5a3-5db3-4fe0-aca3-3e759f8c659e/?context=1000522) (similar).* ***26****. (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522)18 U.S.C. § 2701(c) (https://advance.lexis.com/api/permalink/96555f1c-dffc-4add-832b-7b92cd5912be/?context=1000522).* ***27****. (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522)18 U.S.C. § 2702(b) (https://advance.lexis.com/api/permalink/0243a35b-2026-45f3-ae4f-dc4bd3b143bd/?context=1000522).* ***28****. (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522)In re Facebook Privacy Litig., 791 F. Supp. 2d 705, 714 (N.D. Cal. 2011) (https://advance.lexis.com/api/permalink/241cd3ae-98f7-4bf2-ba7c-772cb9efc953/?context=1000522), rev'd on other grounds, (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522)572 Fed. Appx. 494 (9th Cir. 2014) (https://advance.lexis.com/api/permalink/8a3ff699-6449-4984-8325-533b700eaadf/?context=1000522); (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522) In re Am. Airlines, Inc., Privacy Litig., 370 F. Supp. 2d 552, 560–61 (N.D. Tex. 2005) (https://advance.lexis.com/api/permalink/a9c01650-6eae-4663-a893-6c7ce752a00d/?context=1000522).* ***29****. (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522)18 U.S.C. § 2702(c) (https://advance.lexis.com/api/permalink/0243a35b-2026-45f3-ae4f-dc4bd3b143bd/?context=1000522).* ***30****. (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522)18 U.S.C. § 2703(e) (https://advance.lexis.com/api/permalink/e0be6a77-bee2-443a-a88d-9c216d9d29a5/?context=1000516).* ***31****. (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522)18 U.S.C. § 2702(c)(4) (https://advance.lexis.com/api/permalink/0243a35b-2026-45f3-ae4f-dc4bd3b143bd/?context=1000522).* ***32****. (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522)18 U.S.C. § 2707(e) (https://advance.lexis.com/api/permalink/6b9ae986-9ac9-4813-9760-04781c352731/?context=1000516).* ***33****. See (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522)Sams v. Yahoo! Inc. 713 F.3d 1175, 1179–1181 (9th Cir. 2013) (https://advance.lexis.com/api/permalink/ab9577e6-62ef-47f3-9e82-ae4a16f5c7f1/?context=1000522).* ***34****. See (https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522)Sams v. Yahoo! Inc. 713 F.3d 1181 (https://advance.lexis.com/api/permalink/ab9577e6-62ef-47f3-9e82-ae4a16f5c7f1/?context=1000522);*

(https://advance.lexis.com/api/permalink/b04b2cdc-d385-4b23-99f1-c5beea0945bb/?context=1000522) McCready v. eBay, Inc., 453 F.3d 882, 892 (7th Cir. 2006). ***35****. Compare (https://advance.lexis.com/api/permalink/981b5c23-7d67-41a8-961e-8529d8596f18/?context=1000522)Van Alstyne v. Elec. Scriptorium, Ltd., 560 F.3d 199, 206 (4th Cir. 2009) (https://advance.lexis.com/api/permalink/6076b3df-9e1b-41f5-890e-44530bf0bf51/?context=1000522) (actual damages are a prerequisite to recover statutory damages) with (https://advance.lexis.com/api/permalink/981b5c23-7d67-41a8-961e-8529d8596f18/?context=1000522)Shefts v. Petrakis, 931 F. Supp. 2d 916, 918 (C.D. Ill. 2013) (https://advance.lexis.com/api/permalink/e2574679-18f1-4850-8639-06efa7cc0aa5/?context=1000522) no actual damages necessary to recover statutory damages).* ***36****. See (https://advance.lexis.com/api/permalink/981b5c23-7d67-41a8-961e-8529d8596f18/?context=1000522)Council on American–Islamic Rels. Action Network, Inc. v. Gaubatz, 891 F. Supp. 2d 13, 26–27 (D.D.C. 2012) (https://advance.lexis.com/api/permalink/081da066-f948-4226-a112-f8ef1a3ab2d0/?context=1000522); (https://advance.lexis.com/api/permalink/981b5c23-7d67-41a8-961e-8529d8596f18/?context=1000522)Garback v. Lossing, 2010 U.S. Dist. LEXIS 99059, at *19 n. 6 (E.D. Mich. Sept. 20, 2010) (https://advance.lexis.com/api/permalink/57454f47-a6ec-4bec-af42-4460344d2239/?context=1000516); (https://advance.lexis.com/api/permalink/981b5c23-7d67-41a8-961e-8529d8596f18/?context=1000522)Jones v. Global Info. Grp., Inc., 2009 U.S. Dist. LEXIS 23879, at *5–7 (W.D. Ky. Mar. 25, 2009) (https://advance.lexis.com/api/permalink/10d54986-7600-4828-b6a1-f4b8e512ce3e/?context=1000522). (https://advance.lexis.com/api/permalink/981b5c23-7d67-41a8-961e-8529d8596f18/?context=1000522)*

Technology Tools to Tackle Tax Evasion and Tax Fraud

OECD

BETTER POLICIES FOR BETTER LIVES

Photo credits: all images courtesy of Shutterstock.com

Table of contents

Executive summary

While most taxpayers comply with their tax obligations, some are determined not to. Tax evasion and tax fraud continues to occur and can be substantial, amounting to many billions per year. Not only is this against the law and defrauds the government of revenue, but it also creates an un-level playing field for compliant taxpayers.

Many tax authorities around the world are seeing particular types of tax evasion: under-reporting of income through electronic sales suppression and over-reporting of deductions through false invoicing. Tax evasion and fraud can be further facilitated by the cash economy and the sharing (or online) economy.

However, cost effective technology solutions are already available for tax authorities to implement, and which prevent and detect these types of tax evasion and tax fraud.

This report draws on the experience of 21 countries in this area, including several developing countries, and highlights their key successes in using these technology tools. Not only has substantial tax revenue been raised due to the reduction in tax evasion and tax fraud, but where these solutions have been implemented; a deterrent effect is shown, with overall increasing compliance by taxpayers.

This report has been prepared with a view to encouraging other tax authorities to consider whether the same approach may be effective in their jurisdiction. It is the second in a series of reports focusing on the use of technology and digital solutions to address tax evasion, the first being the report *Electronic Sales Suppression: A threat to tax revenue* (OECD, 2013).

This report is divided into four key parts:

- ***Electronic sales suppression and counter-technology:*** the problem, the key features of available technology solutions, the proven benefits as well as the costs, and the complementary actions needed to implement such solutions;

- ***False invoicing:*** the problem, the key features of available technology solutions, the results and benefits, and the complementary actions needed to implement such solutions;

- ***The cash economy and the sharing economy:*** the challenges posed by these segments of the economy and the work tax authorities are doing to address the cash and sharing economy; and

- ***Best practices:*** the lessons from other tax authorities as to how these technology solutions can be effectively implemented.

The annexes to the report contain a more detailed technical catalogue of the technology solutions being used by tax authorities to address electronic sales suppression and false invoicing. To increase the potential for sharing of experience between tax authorities on the solutions they are using, the OECD Secretariat can also provide contact details for tax authorities to follow up on particular solutions contained in the report.

Chapter 1

Introduction: A compelling case

Chapter 1

Introduction: A compelling case

Tax evasion and fraud is illegal and intentional misrepresentation of tax obligations. It can involve deliberate omission or falsification of income or revenue, as well as efforts to be invisible to tax authorities altogether. This results in the reduction of income that lawfully belongs to the government, and to the people. The loss of income can be substantial; for example, a study by European Commission reported that the total VAT Gap for 26 EU countries amounted to approximately EUR 193 billion in the year 2011 alone.

Tax evasion and tax fraud not only cheats the public of revenue that is to be used for public goods, but also puts compliant taxpayers that obey the law at a disadvantage. It makes it harder for those compliant businesses to be profitable when they are competing with businesses that do not bear the expense of paying their fair share of taxes.

Two particular types of tax evasion and tax fraud appear to be widespread in their use: underreporting of income through sales suppression and over-reporting of deductions through false invoicing. These are simple for criminals to achieve and can affect countries of all sizes. These types of tax evasion and fraud can be further facilitated by the cash economy and sharing economy. The impact of this tax crime is huge, with anecdotal evidence alone indicating that it amounts to many billions of dollars in lost tax revenue.

In the past, underreporting of income and over-reporting of deductions were difficult and time consuming for tax authorities to detect. This is changing. Many tax authorities are now using technology solutions to detect these tax crimes. These solutions have been effective, and these tax authorities are making progress in bringing previously undetected and lost income into the revenue base, in a way that is also resource efficient for the tax authority. As more solutions become available in the market and the costs reduce, tax authorities have an opportunity to prevent and detect crime, significantly improve their revenue collection and increase the efficiency of their operations.

For this reason, the Task Force on Tax Crime and Other Crimes (TFTC) called for a report to publicise the importance and effectiveness of technology solutions that are being used to detect tax fraud and evasion. This report was based on survey responses and discussions with 21 tax authorities[1] on the solutions they are using or putting in place, as well as publicly available information and consultation with the private sector providers of the relevant technology solutions.

1. Information received from Argentina, Australia, Austria, Belgium, Canada, Finland, France, Germany, Ghana, Greece, Hungary, Italy, Kenya, Mexico, the Netherlands, the People's Republic of China, Rwanda, Singapore, Slovak Republic, Sweden, and the United Kingdom.

This report is not intended to be a comprehensive picture of all technology solutions being used by tax authorities around the world. Rather, it gives a clear picture of the direction that a number of tax authorities are taking, and should lead to further work on sharing information on other technology solutions as they emerge.

The report is divided into two sections. The first provides a brief overview of the types of technology tools that tax administrations have implemented to address tax evasion and tax fraud problems. Looking first at electronic sales suppression and then at false invoicing, it describes the problem, the key features of the technology solutions being used to address the problem, the results, and the complementary tools used to implement the solutions. The report then considers complementary work that is being undertaken to address the cash economy and sharing economy, which, although not types of tax evasion and fraud themselves, can facilitate it.

Table.1.1 Chart of solutions contained in this report

Problem	Sector	Solution	Report Reference
Under-reporting of income	Business – to – consumer *e.g.* restaurant, bars, taxi, convenience store	Data recording technology in electronic cash registers / sales machines	Chapter 2 and Annex A
Over-reporting of deductions	Business – to – business *e.g.* construction	Electronic invoicing and automated reporting	Chapter 3 and Annex B
Lack of visibility of business activity	Cash and sharing economy	Legal, policy and analytics	Chapter 4

The second section in Annexes A and B is a more detailed catalogue of the technology solutions being used to address electronic sales suppression and false invoicing, with a view to allowing other tax administrations that are facing the same types of challenges to draw on that experience.

The report concludes that the case for the use of technology to assist in countering tax fraud and evasion is compelling. To make the best use of these available tools, tax authorities must continue to be proactive in sharing experience in order to stay abreast of the tax evasion and fraud techniques as they continue to evolve.

Chapter 2

Electronic sales suppression and counter-technology

Chapter 2

Electronic sales suppression and counter-technology

At a basic level, sales suppression can be as simple as not recording some cash sales with the intention of under-reporting the amount of sales and thereby under-reporting the corresponding tax liability. However, more sophisticated methods have become very prevalent. With the increased use of technology in businesses, and the increased use of electronic payment forms such as debit cards, sales suppression is also being undertaken through electronic tools that can alter evidence of transactions whether paid in cash or card, without leaving a trace of the alteration. These transactions can also be underreported by using the cash register in training mode, or cancelling transactions after they have occurred. Without the correct data, tax authorities cannot assess the correct tax.

In the past, sales suppression could be achieved simply through putting cash straight into your pocket or editing the accounting books. Now, sales suppression has become more sophisticated through the use of technology which makes it much harder for administrations to detect. The two main electronic sales suppression tools that are used are phantomware and zappers.

Phantomware involves the installation of software as part of the sales register. It allows a program to operate on the sales register which can alter the data that has been recorded. The program is only accessible through a hidden menu which allows the business owner to covertly manipulate the sales records after the transaction has occurred.

A zapper is an external device or external program accessed online that can be connected to the cash register. When connected to a cash register, it allows the manipulation of transaction records, performing a similar function to phantomware.

Both phantomware and zappers allow the user to delete individual sales records altogether and also to substitute the sales amounts to a lower figure and thereby reducing the overall sales. Because of their concealed nature, the cash register appears to users to operate normally and poses a challenge to tax auditors to detect.

New sales suppression techniques have emerged. Referred to as “sales suppression as a service”, this tool allows a taxpayer to achieve sales suppression through a foreign zapper which operates over the internet. The service provides deletion, alteration and replacement of sales data or remote crashing of the hard drive. This can be very difficult for the tax authority to detect as it otherwise appears authentic, or appears not to be attributable to any actions of the taxpayer. Often the service provider is in a foreign jurisdiction, making it difficult for domestic authorities to take enforcement action.

What solutions can address electronic sales suppression?

Where tax crime is facilitated by technology, a technology response is needed. The most common counter-suppression tool used to address electronic sales suppression is data recording technology. This tool records and secures the sales data immediately as the transaction occurs and stores it in a manner that means it is tamper proof. This means it cannot be manipulated by phantomware or zappers, or if tampering has occurred, it is traceable and detectable. The data should be stored securely and preserved even if there is loss of power.

There are different types of tools that are being used to perform this function, which are referred to in different countries and by different service providers as a fiscal control unit, electronic fiscal device, fiscal memory device, sales data controller or sales recording module. This type of technology should be able to be used in any type of cash register, such as traditional electronic cash registers (ECRs), computer-based point of sales systems, or those that are tablet or smartphone-based. Different solutions are available which can either be included as an integrated part of a cash register, or as an add-on installed with an existing cash register.

As an additional feature, these types of tools are also being used to send data automatically to the tax authority, connecting cash registers online to their data server systems. This can occur either in real time or in bulk scheduled transfers, such as at the end of the day or each month. The tax authority then has the opportunity to access the data remotely for compliance and audit purposes.

What are the results and benefits?

Results from these devices have been impressive their ability to bring previously untaxed amounts into the revenue base.

In Hungary, electronic cash registers increased VAT revenue by **15%** in the concerned sectors.

Box 1. Highlights of results from electronic data recording technology

In Austria, results from the electronic sales suppression tools are expected to be an additional EUR 900 million in tax revenues.

In Belgium, initial comparisons shows an 8% increase in restaurant sales reported after installation of their solution as with sales reported before.

In Quebec in Canada, At 31 March 2016, CAD 1.2 billion (EUR 822 million) in taxes was recovered following the introduction of sales recording modules into the restaurant industry. Projections are that, by 2018-2019, this will cumulatively amount to CAD 2.1 billion (EUR 1.44 billion). In addition to tax losses, in 2008 the Canadian Revenue Agency criminally charged the owners of four restaurants with tax evasion involving the "zapping" of nearly 200 000 cash transactions, totaling EUR 3.1 million.

In Hungary, electronic cash registers were installed with a fiscal control unit. After the first year of operation, VAT revenue increased by 15% in the concerned sectors. The increase in VAT revenues has exceeded the overall costs of the project of introducing the new systems.

In Rwanda, electronic cash registers were introduced in March 2013. In 2015, VAT collected on sales had increased by 20%.

In Sweden, since 2010, 135 000 cash registers are connected to a fiscal control unit. This includes all companies selling goods and services paid in cash. Increased VAT and income tax revenues has been estimated to around SEK 3 billion (EUR 300 million) per annum since the legislation was implemented. The legislation has also led to better control measures for the Swedish Tax Agency.

There are also benefits for businesses. For instance, tools that prevent the manipulation of sales data and ensure secure accurate reporting will also protect from theft by employees. In addition, tools that accurately record and store data and share it with the tax authority can reduce the burdens of an audit for both the tax authority and the taxpayer.

For example, in the province of Quebec the time required to audit a restaurant used to take 70 hours, but after the introduction of their sales recording module, it now takes three hours. This allowed the tax authority to significantly increase the number of inspections from 120 to 8000 per year. This can be beneficial for business, as the audit can occur electronically and remotely rather than at the business and requiring the production of volumes of hard copy documents, meaning reduced time and interruption to the business.

What features do these solutions have?

Common regulatory and design features of these solutions include:

Table 2.1 Key features of data recording technology solutions

Feature	Benefits
Regulation and certification of cash registers	Ensures that the cash registers that are authorised for use are only those that have the requisite functions (and do not have prohibited functions that allow sales suppression). One mechanism for doing this is to license only certain market vendors of cash registers. Another mechanism is to introduce regulations that detail the specifications that must be present in cash registers, and allowing the market to provide solutions that meet these requirements.
Data content requirements	Prescribing the details of what data must be recorded and printed on the purchase receipt ensures that the information is useful to the tax administration for verification and for compliance action. This data can be defined as fiscal data and can include the amount of the sale, amount of VAT / sales tax due, time, date, invoice number, the mode of operation that the register was in (such as training mode), and the type of receipt (such as refund or a non-final bill in a restaurant).
Data security: Digital signature of receipt	A digital signature or a control code provides a unique identifier with the details of the transaction such as date, time and amount of the transaction. The digital signature or control code is stored with the transaction data and also printed on the customer's receipt. The signature can be encrypted or a certificate e-signature, for which the tax authority has the corresponding key to identify the creator of the data. Digital signatures allow each transaction to be traced and verified, because the unique identifier guarantees that the data has been generated by the particular taxpayer and has not been altered since the signature was created. If the transaction is subsequently altered, a different digital signature identifier will be generated, leaving a trace of the change.
Data storage	Data must be stored separately and securely from the cash register in a tamper proof environment to prevent manipulation or hacking. The data should be stored at the point the transaction occurs. The data can be stored on an external device that is connected to the cash register (a "black box"), fully integrated inside the cash register or the receipt printer (such as a microchip or sim card), or connected to and stored in cloud-based solutions.
Online data accessibility: Remote access by the tax administration	Where the tax authority has remote access to the information at any time, it deters taxpayers from subsequently altering records. It also allows the tax authority to use the data for audit case selection and in compliance activities, and may make such activities more efficient as the data is already available without having to send a specific request or attend an on-site audit examination. This also assists tax authorities where data may otherwise be stored offshore which can pose challenges for audit.
Data transmission: Reporting to tax administration	Regular data transmission of the records to the tax authority deters taxpayers from altering records as they know the tax authority will have direct data. Information exchange with the tax office can be in real time or at periodic intervals. As online automatic transmission relies on Ethernet or GSM net connectivity, periodic uploading through mobile online devices with secure data buffering capabilities may be suitable in places where reliable connectivity is not in place, and may in some cases be more manageable for the tax authority. It also allows the tax authority to use the data for audit case selection and in compliance activities, and may make such activities more efficient as the data is already available without having to send a specific request or attend an on-site audit examination. This also assists tax authorities where data may otherwise be stored offshore which can pose challenges for audit.

The above described features can be combined in a counter-suppression technical solution in different ways. Important aspects to consider when choosing a solution is the degree of data security (encryption or e-signing) and tamper proof storage; whether to store the secured fiscal data in an external add-on device (a fiscal box) or fully integrated as a module inside the cash register. Requiring certification of solutions and cash registers will simplify and enforce compliance.

A more detailed summary of solutions implemented by some countries is included in Annex A.

What are the costs?

A key factor in making a technology choice that will be as affordable, effective and easy to implement as possible is to assess the structure of a jurisdiction's cash register market, in particular the range of cash registers in use in different market sectors, from traditional simple cash registers to more sophisticated point of sales equipment. This can make it easier to determine how many cash registers could be upgraded or replaced and the technology price range accordingly.

Costs of these types of solutions have been decreasing over time. Many solutions being used are off-the-shelf solutions that can be installed by the taxpayer, or are already installed in certified cash registers. Factors that can affect the costs of the solution include the degree of modification required to existing machines (as modification of existing systems can be more expensive than adding on a separate component), the size of the market that is implementing the solution, and whether the solution is procured through the open market. Although it is difficult to generalise, costs can be as low as under EUR 30 and up to around EUR 1 000.

The costs to the tax authority should also be considered. This should include giving consideration to the most effective means of enforcing the implementation of the technology solution, including the extent to which the tax administration is itself responsible for technical aspects such as certifying individual cash registers, or inspecting bespoke modifications to existing machines. In addition, the costs for the tax authority of either remotely accessing or receiving and storing bulk transaction data should be considered. In either case, automated data analytics tools could be considered to detect patterns, anomalies or gaps, which would reduce the costs of detecting any unusual results.

What other actions are needed to implement the solution?

The degree and type of other tools needed to implement data recording technology solutions may depend on the domestic legal framework, such as the regulatory power of the tax authority and the extent to which there is evidence of electronic sales suppression in the country that justifies the introduction of mandatory technology tools. In most cases,

the legal framework will be at the heart of any solution. Additional tasks that should be considered when introducing a technology tool include consultation with taxpayers and the private sector, incentives to taxpayers, legislation and regulatory, as well as monitoring and enforcement. These tools can be used in conjunction and are not mutually exclusive. Further examples on each are included below.

Figure 2.1 Key building blocks to implement the solution

- ***Legislation*** to require the production of invoices for every transaction, together with legislation requiring the use of data recording technology or cash register that are compliant with specified standards. The technical requirements should be very clear and its implementation easily able to be verified. Legislation can also specify how cash registers should be used, such as prohibitions on using cash registers in training mode which prevents transactions being recorded or providing restrictions on how refunds should be recorded to ensure transactions are not falsely reversed as a refund where the taxpayer keeps the payment.
  Examples: Austria's Fiscal Procedure Code, Sweden's Cash Registers Act.

- ***Consultation and collaboration*** with taxpayers and the providers of cash registers is beneficial when defining the appropriate standards.
  Examples: the Netherlands worked with the industry to develop a set of "quality marks" which are indictors of reliable cash registers. The state of Ontario in Canada is undertaking a public consultation with businesses and others to obtain input on technology solutions can address electronic sales suppression, in ways that minimise the burden for industry.

- ***Incentives*** for business to voluntarily install data recording technology, such as an enhanced tax deduction, subsidised costs or linking the use of compliant cash registers to a reduced likelihood of audit.
  Examples: Austria provides a special tax deduction upon the taxpayer reporting to the tax authority that they have installed the required device. Experience has shown that even where the government pays for the systems to be used, this is paid for very quickly in the revenue results.

- ***Compliance awareness among customers*** such as a receipt lottery. This encourages awareness amongst the public of the risk of tax evasion and tax fraud through the misuse of invoices, and enables them to act as an enforcement mechanism, giving taxpayers a business incentive to comply. An extra incentive can apply where customers can enter their receipt into a lottery or accumulate points for each receipt submitted, giving them a chance to win a prize.
  Examples: Colombia and Portugal.

- ***Monitoring*** the introduction of the new technology. This can include requiring suppliers of the cash registers to report to the tax authority to certify that their products meet the specifications, and / or requiring taxpayers to report when they have installed a compliant data recording technology device. The tax authority could then maintain a register or database to assist in follow up audits.
  Example: In Sweden a person possessing a cash register must report this to the tax authority, and each cash register has a unique identification number.

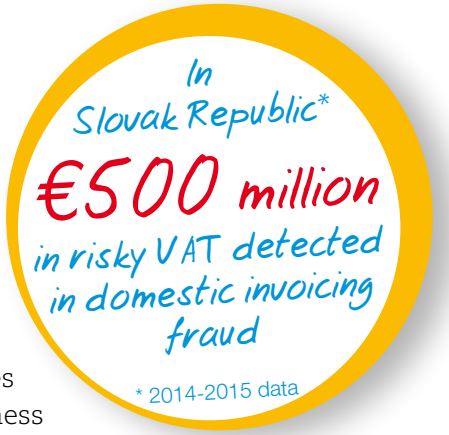
- ***Enforcement,*** such as legislation and penalties for using or distributing electronic sales suppression devices to deter and penalise both the use and the supply of sales suppression technology.
  Examples: almost 20 states in the United States have enacted such legislation. This must be supported by effective audit strategies to detect non-compliance with the requirements and ability to enforce penalties.

Chapter 3

False invoicing

Chapter 3

False invoicing



What is the problem?

Whereas sales suppression techniques seek to under-report revenue, false invoicing seeks to over-report deductions, and to falsify invoices to mask non-deductible personal expenses as legitimate deductions. False invoicing occurs where a business fabricates or inflates invoices which name the business as the debtor. This allows it to fraudulently claim expenses for tax purposes that have not been incurred. Although in theory a tax authority can verify the validity of each invoice by comparing it to the records of the counterparty to the transaction, it is time consuming and resource intensive to do so.

Box 2. Estimated impact of false invoicing

Between 2007 and 2009 Mexico lost just under EUR 3 billion in tax revenue due to forged invoices.

In the Slovak Republic, during the years 2014 and 2015 the amount of risky VAT detected in domestic invoicing fraud was more than EUR 500 million.

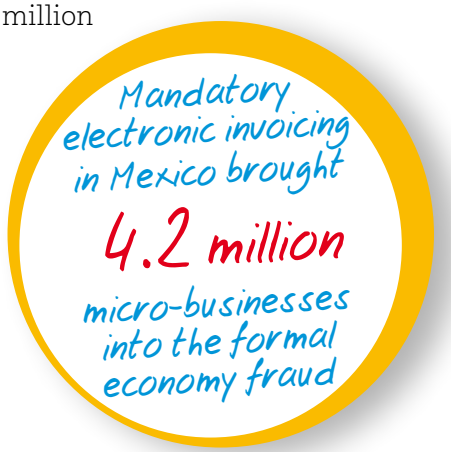
What solutions can address false invoicing?

A solution to address the problem of false invoicing is requiring electronic invoicing. Generally businesses must retain records of transactions with customers and provide an invoice to a customer, either in electronic or paper form. An electronic invoice documents the transaction in electronic format. The electronic invoicing system should have additional features to ensure the integrity of the data and the identity of the creator. This can be done by using a digital signature to ensure authenticity of the invoice and that it has not been altered after its creation.

Electronic invoicing will be most effective where the invoices must be registered or otherwise provided to the tax authority. The detection of false over-reporting of deductible expenses can be achieved by automatic matching of the data for the purchaser and seller. Where this is undertaken through periodic or real time data transfers, the tax authority has substantially enhanced visibility of its taxpayers, and can perform audits, analytics and tax return functions in an efficient way.

What are the results and benefits?

Electronic invoicing has been implemented in a number of countries, with evidence beginning to be collected on its impact. For example, Argentina, Bolivia, Brazil, Colombia, Costa Rica, Ecuador, Guatemala, Italy, the People's Republic of China, Peru, Rwanda and Uruguay have implemented electronic invoicing. The impact in Mexico alone was that mandatory electronic invoicing in Mexico brought 4.2 million micro-businesses into the formal economy.



Electronic invoicing can have the additional benefit of replacing paper invoices, eliminating the need to print, send and store invoices. Recognising the substantial cost savings that arise, the European Union introduced standardised electronic invoicing (Directive 2014/55/EU) for use in public procurement.

What features do these solutions have?

Common features of electronic invoicing are shown in Table 3.1.:

Table 3.1 Key features of electronic invoicing solutions

Feature	Benefits
Standardising the requirements of electronic invoices	Specifying the requirements such as the content or format, or certifying the providers of electronic invoicing solutions gives quality assurance and ease of audit. It also makes the widespread introduction of electronic invoicing clear and consistent for businesses. Where one standardised format is required, this can make the automatic processing and analysis of bulk data easier for the tax authority.
Digital signature of receipt	Signature provides a unique identifier with the details of the transaction such as date, time and amount of the transaction. The tax authority has the matching key to decrypt the signature and can determine if the receipt is complete and authentic. If the transaction is subsequently altered, a different digital signature identifier will be generated, leaving a trace of the change. Using a digital signature is therefore an important aspect of also being able to verify invoices.
Connection of electronic invoicing to sales recording device	This gives assurance that the invoices are correct when created, and that the data is correctly stored and tamper-proof.
Provision of invoice information to the tax authority	The information generated through electronic invoicing can be provided to the tax authority. This can be by requiring the transmission of all invoices, or specifying the summary information to be transmitted. This could be in real time through online connection to the tax authority, or at scheduled intervals.

What other actions are needed to implement the solution?

As with electronic sales suppression, technology is not a standalone solution, but features as part of a package. To make the introduction of electronic invoicing effective, the following complementary features have been used:

- ***Legislation*** requiring electronic invoices, supported by penalties for failure to do so. This could be supported by legislation allowing the tax authority to access third party data to match payment flows to taxpayers.

- ***Online verification tools***. Example: in Argentina, after the transaction is approved the taxpayer has to apply to the tax authority for authorisation. If the invoice contains the required information, it is authorised as valid and has fiscal effects against third parties. The information is kept in the database of the tax authority which can be used to subsequently cross-check other tax reporting and collection. In addition, third parties can access a verification tool online, in which they can enter the details of the invoice they have received and instantly verify that it matches the information already registered with the tax authority and therefore know whether it can be relied upon for tax and other purposes.

- Aligning the requirements for the format and content of the electronic invoices to other ***tax record keeping and reporting obligations***, or using it to pre-fill returns, can streamline the compliance burden for businesses. Another approach that has been used is to provide relief from tax penalties in the event of an audit provided that the business has implemented the required invoicing tool.

- ***Incentives*** for taxpayers, such as providing software to assist. Examples: in Italy the Revenue Agency is making software available to businesses for free from July 2016 to conduct electronic invoicing in business to business transactions enabling the operators (especially the micro-small enterprises) to create, transmit and store the electronic invoices. In Chile, the government provides online accounting software which allows small businesses to record transactions and generate pre-filled tax returns. Negative incentives can also be used, such as making the use of electronic invoicing a requirement for the business and the customer to be entitled to claim a deduction in respect of certain transactions or claim input credits for value added taxes. Example: in Italy, the option to electronically transmit invoices would relieve the taxpayer from existing reporting obligations, which is expected to significantly reduce the compliance burden for taxpayers.

Since taxpayers are generally required to maintain business records, the introduction of electronic invoicing may not be a significant departure from existing obligations. Where businesses are currently using paper based record keeping, the introduction of electronic invoicing can bring benefits of greater accuracy and efficiency, particularly where the electronic invoicing system can be used to easily fulfil other tax compliance obligations.

A more detailed summary of solutions implemented by some countries is included in Annex B.

Chapter 4

The cash economy and the sharing economy: Complementary work to address the risks

Chapter 4

The cash economy and the sharing economy: Complementary work to address the risks

What are the challenges posed by the cash economy?

The cash economy and the sharing economy, while not forms of tax evasion or fraud *per se*, have features that can facilitate tax crime. As such, the work that is being undertaken in this area can have a complementary impact on the effectiveness of the technology solutions described above.

The features of the cash economy that can facilitate tax crime are that cash is fungible and untraceable. This makes it easier for under-reporting and falsification to occur as there is not necessarily a record trail as there might be when credit and debit cards and electronic funds transfers are used. The solutions identified above - using tamper proof data recording technology and requiring electronic invoicing - will work together to reduce the risks posed by the cash economy.

What work is being undertaken to address the cash economy?

Tax authorities are working on a range of solutions, including legislation, analytical tools and encouraging the use of cashless payments such as mobile phone payment methods.

Box 3. Examples of other approaches to address the cash economy

In Argentina, a partial reimbursement of VAT is offered for purchases of personal property or hiring of services when the final consumers perform the transaction using authorised credit card or bank transfers.

In Austria, legislation provides that cash payments for services in the construction industry (including labour) exceeding EUR 500 are no longer tax deductible. The payments must be performed via bank transfer in order to claim the deduction, and this is auditable. Payments for wages for work in the construction sector must not be afforded or accepted in cash if the employee has a bank account or legitimate claim for one.

In Finland, ATM withdrawals are monitored. Withdrawals are summarised by credit / debit card number and cardholders are identified by card number (domestic issued cards) or other means (cards issued abroad). A photograph is taken at the ATM to identify the person withdrawing the cash, and this is available to the tax authority through online connection. If necessary, the photograph will be used for identification purposes at a later stage and this can be used as a risk indicator and / or in conjunction with other information during an investigation.

Box 3. Examples of other approaches to address the cash economy *(continued)*

In France, limits are imposed prohibiting cash payments over EUR 1 000.

In Greece, limits are imposed prohibiting cash payments over EUR 1 500.

In Italy, restrictions on cash were put in place in the real estate sector. In order to obtain allowances for refurbishment expenses and for energy efficiency improvements to buildings, the payment must be performed through a bank or postal transfer. A withholding tax of 8% is also applied. This system reduces the risk of untraceable transactions but also has an immediate revenue impact.

In Sweden, companies can refuse to accept cash payments. This approach is already being used by some restaurants, public transportation and hotels. In Sweden the use of cash is decreasing, and approximately 80 % of all transactions are made electronically, including through new techniques such as smartphones and contactless payment methods. An app developed by banks in Sweden facilitates money transfers between private persons and make payments to companies, which has increased in use from 76 000 transactions in 2012 to 76 million transactions in 2015.

What are the challenges posed by the sharing economy?

While the cash economy has long been considered by tax authorities, the sharing economy is a relatively new issue. A number of tax administrations have started to investigate the risks of tax evasion and fraud posed by the sharing economy. This includes businesses that operate online through community marketplaces, such as private renting of residential premises through sharing platforms such as Airbnb, driving services through online platforms such as Uber and professional selling through online platforms such as eBay. PriceWaterhouseCoopers estimates that the sharing economy generates USD 15 billion in revenue around the world, and this this could grow to USD 335 billion by 2025.

The challenge of the sharing economy that means it can facilitate tax fraud and evasion is that it can be more difficult to identify the existence of business activity. This is particularly true where the person is not registered as conducting a business or is in a foreign jurisdiction. However, the online nature of these platforms also presents an opportunity to deploy technology to tackle this.

What work is being undertaken the sharing economy?

Tax authorities are starting work in this area, including analytics, regulatory and policy considerations. In addition, legislative solutions and international co-operation amongst tax authorities is likely to be of assistance in this area, particularly where online platforms are located in jurisdictions other than the location of the customer. For example, the country in which an online platform is situated could introduce requirements that online platforms keep records of its users, which could be reported to the tax authority and exchanged internationally pursuant to information sharing agreements.

Box 4. Examples of approaches to address the sharing economy

Argentina has introduced a special registration system for VAT purposes. This applies to the operator of online portals used for sales operations of new personal property, and online portals where the hiring of services is agreed or performed electronically. The operator of the online portal is obliged to act as VAT collection agents in respect of the transactions performed through the online portal.

Australia makes extensive use of third party data. The tax authority has access to information held in the Australian Transaction Reports and Analysis Centre (AUSTRAC) which is Australia's financial intelligence unit with regulatory responsibility for anti-money laundering and counter-terrorism financing. Through this information, it has traced funds flowing to drivers and renters from overseas to local banks from where they are distributed. The tax authority is using its powers to obtain data from these banks to identify unregistered business activity such as Uber drivers. So far it has been able to identify a large portion of drivers. In addition, the tax authority is working with the platform facilitators, Uber and Airbnb in particular, to have taxation information provided to their partners (i.e. drivers and letters of properties).

Austria uses internet monitoring using different internet scraping tools (web harvesting or web data extraction), some of which are open source and others are custom-made tools. The results of this work feeds into compliance measures such as letters to presumptive taxpayers and information campaigns. Compliance efforts targeting foreign companies offering goods or services in Austria led to VAT collection of EUR 10 million, as well as 44 voluntary declarations resulting in collection of VAT of EUR 5.5 million.

Belgium is using internet scraping and requesting all digital data to enable data mining with existing taxpayer files. This is used in conjunction with other analytics tools such as a 'Forensic Toolkit' to collect and cull data in a forensic inspired way; using Accounting Command Language to analyse semi-structured data which allows importing data from different accounting packages to create a 'standard audit file' and to perform some standard checks; and using an e-discovery solution Zylab to analyse unstructured data like e-mail and PDF documents to search and review this data.

The province of Ontario in Canada is recognising the economic potential of the sharing economy by partnering with Airbnb to launch a new pilot project. Airbnb will educate its hosts through an email notification during tax season to remind them of their tax obligations. The province of Ontario and Airbnb have collaborated to create a webpage with content specific to Ontario regulations.

Finland has legislation to enable the collection of third party information. In addition to audits to collect data to identify shared economy actors, legislation is now used to monitor online credit / debit card payments to detect unregistered remote sellers and VAT EU distance sellers. Data is filtered and clustered by using scripts. Where a significant volume of payments are identified as being made to an unknown person, this can be investigated to determine if the person is an unregistered business. To date, the tax authority has identified 188 unregistered distance sellers, amounting to sales of EUR 50 million. Based on sales, the estimated VAT loss is EUR 12 million yearly.

Box 4. Examples of approaches to address the sharing economy *(continued)*

Japan gathers and analyses information on information-providing services on the internet such as fee-charging websites to identify suspected online businesses, using a general search engine After picking up a specific suspicious company, comprehensive information is collected using internet crawlers which enable an exhaustive search on the internet. Thus, a variety of materials and information is collated in a database and matched against taxpayers in the system of the tax authority. This matching system enables the tax authority to visualise the risks for each taxpayer.

The United Kingdom is using a product called COSAIN which automates the collation and filtering of social media and websites. The tool collates profiles, which can be used to monitor the trends within a geographic area or specific business sector. In future the e-commerce sector will be able to be analysed, such as collating data from sites such as Craigslist, eBay and Gumtree.

Chapter 5

Introducing technology tools: Best practice approaches

Chapter 5

Introducing technology tools: Best practice approaches

The experience of tax administrations in introducing a technology solution shows that there are best practices that can assist in making the implementation swift and effective.

First, as there are a variety of solutions available for any given problem, it is critical that the ***tax administration has clearly defined its objective***. This includes careful identification of the problem that is being addressed, comparing the options available to it, investigating the technology solutions and preparing an implementation plan that is transparent to the taxpayers. It may also be helpful to seek the input of a range of government stakeholders, including policy, budgetary, tax, technical and legislative functions.

Engagement and ***consultation with the taxpayers*** that will be affected is an important aspect of implementing a new solution. This can equip the tax administration with insights into the most cost effective solutions, the solutions that would be suitable for different types, maturity and sizes of businesses, provide an opportunity to resolve questions, provide guidance and identify if other supporting measures (such as incentives or enforcement measures) may be needed to bring about swift change. Framing this dialogue in a positive manner can be particularly effective, as although there may be costs for taxpayers there is an opportunity to present the benefits for taxpayers. This includes the importance of ensuring a level playing field between competitors, the ability to streamline other tax reporting obligations, and the ability to guard against reputational damage that arises from tax crimes.

Collaboration with the private sector providers of the solutions from an early stage can be helpful if the market will be supplying the relevant technology solution, and market competition in this field can reduce the costs for taxpayers. Early engagement with the private sector can also assist the tax administration in learning the technical terminology and equipping it to accurately describe the required specifications. This can in turn ensure that the private sector understands how to meet the requirements. Engagement with the private sector can also assist in designing a solution that will be future proofed; for example, to ensure that any updates in software or improvements in the design are able to be implemented in a cost effective manner over time rather than requiring substantial and repeated investments. Testing prototypes of technology test or practical proof of concept evaluations can further support the development of relevant technology requirements and specifications, which ultimately facilitates efficient implementation.

In some cases, tax administrations have adopted a ***pilot project approach***. This approach can introduce the solution for an initial test period, such as in a particular region or a particular business sector which is at high risk of tax fraud and evasion, or introducing

it as a voluntary solution coupled with an incentive for businesses that participate in the pilot project. This can be helpful in identifying any implementation problems or unforeseen practical questions. Once any implementation problems have been resolved, the solution can be implemented more widely in industry sectors or locations which are the next priority in terms of risk.

Harnessing the deterrent effect is also an important aspect. This can be done by efforts to raise the public awareness of the extent of the problem, which can mean that the public is an important advocate of change. This can be particularly helpful if legislative changes will be used to introduce a technology solution. Campaigns can be continued over time to publicise the results of technology solutions in recovering public revenue, as these boost taxpayer morale, reinforce the deterrent effect of these solutions and lend support to further expansion of the use of technology tools in preventing and detecting tax fraud.

Enforcement efforts are also necessary to ensure the effective use of technology solutions. These act as a deterrent for businesses in avoiding or misusing the required technology solution as well as penalising any offenders. In addition to pecuniary penalties, other examples of penalties that are used include the suspension of a business licence, imposing a period of enhanced supervision by the tax authority, and public "naming and shaming" of non-compliant taxpayers. The public can also be encouraged to act as an enforcement mechanism where there is a whistleblowing mechanism, allowing employees or customers to inform the tax authority of suspected violations of tax obligations, and possibly offering a reward for doing so. In order to enforce the requirements, the tax authority will need a mechanism to detect and measure non-compliance, including an ability to measure the correct functioning of a technology solution such as through certification.

Finally, tax administrations should continue to engage with taxpayers, the private sector and with each other in order to stay abreast of new risks and share the gains made in implementing new solutions. Technology is a fast changing area, and criminals will continue to find new approaches that demand new response from tax authorities. Tax authorities should continue to share their experiences and insight in utilising technology to combat and deter tax evasion and tax fraud, as well as provide feedback into the broader reform efforts across the tax administration to improve tax compliance.

Chapter 6

Conclusion

Chapter 6

Conclusion

The results that can be achieved by utilising technology to detect and prevent tax fraud and tax evasion speak for themselves. These solutions can offer a win-win: better detection of crime, higher revenue recovery, and synergies that can make tax compliance easier for business and tax administrations. This short report shows that in many cases working solutions are already in place, and that a number of countries are already able to share their experience in the implementation process. It is hoped that this brief report serves as an encouragement for all countries to consider the risks in their taxpayer segments, and to take advantage of the experience of others included in this report to leverage the lessons already learned.

Technology tools are not a single fix to the problem of tax fraud and tax evasion, but if implemented effectively, substantial progress can be made in high risk areas. These solutions should always be accompanied by the other necessary tools available to tax authorities, including legislative measures, effective enforcement, taxpayer consultation and international co-operation.

This report has focused on just a few areas where technology solutions are having a significant impact. As technology and taxpayer behaviour continues to evolve, further areas of work will become relevant. This could include further work on the sharing economy; carousel fraud; customs fraud. Any further work in this area could also build on the ongoing work in the field of data analytics undertaken by both the Task Force on Tax Crimes and Other Crimes and the Forum on Tax Administration.

Annex A

Catalogue of country solutions for electronic sales suppression

Argentina • Austria • Belgium • Canada (Quebec) • Finland • France • Germany • Ghana • Greece • Hungary • Italy • Kenya • Netherlands • Rwanda • Slovak Republic • Sweden

Annex A

Catalogue of country solutions for electronic sales suppression

Argentina

Electronic cash registers / fiscal printers have been implemented in Argentina since the late 1990s. In December 2013, the requirements were strengthened to incorporate new technology with improved intelligence and security in response to evasion techniques that emerged. The new equipment will generate electronic files of the transactions performed, including a digital signature. The files will be regularly transmitted to the tax authority in a similar mechanism as is used for the filing of tax returns.

For reference, see General Resolution N° 3561/13 AFIP, at www.infoleg.gov.ar.

The challenges that need to be considered in introducing the technology tools include:

- Limitation of the implementation by the taxpayers who are located in areas of the country with low or no internet connectivity;
- Preference for paper procedures in some sectors (mainly small taxpayers or areas within the country);
- Costs that have to be paid by the taxpayers for the adaptation of their invoice systems and/or the acquisition of the equipment;
- Need to detect possible mistakes in the development of taxpayers invoicing systems early.

Austria

Technical features: Changes to the Austrian Federal Fiscal Code were introduced in two tranches.

From 1 January 2016:

- For every transaction a receipt has to be issued.
- Compulsory introduction of electronic cash registers or other electronic recording systems for digital recording business cases and for printing receipts for all businesses with annual turnover of more than EUR 15 000 provided that annual cash turnover exceeds EUR 7 500.
- Each cash register must draw up a data collection log (DCL) to record and store each individual cash transaction. The DCL has to be exportable without delay in case of a request from the tax authorities.

From 1 April 2017:

- A secure signature creation device has to be implemented in the cash register.
- All receipts have to be signed.
- The cash register has to have a cumulative memory, meaning that the transactions recorded in the cash register are added up continuously. The cumulative memory is part of the signature and constitutes another measure for the prevention of manipulation.
- The cash register has to print a monthly final zero-receipt with the level of the cumulative memory and to store it in the DCL

Companies must acquire the required number of signature creation devices from a certified service provider offering qualified signature certificates that is established in the EU, EEA or in Switzerland. The recording-software of the cash register does not have to be certified because the security mechanism consists of linking cash transactions using the electronic signature of the signature creation device. The linking is formed in the signature to be generated by including elements from the last assigned signature saved in the data collection log. When recording the first cash sale, the cash register identification number replaces the last assigned signature.

Enforcement: At the request of the tax authorities, the company must record a cash transaction set to zero and hand over the receipt issued by the cash register for inspection purpose. For cash registers with a device to transmit payment receipts electronically, the receipt must be made available electronically. At the request of the tax authorities, the company must export and hand over the DCL for a period specified by the tax authorities to an external data carrier. The data carrier must be provided by the company.

There are penalties for manipulating cash registers, which apply both to the taxpayers as well as the producers / software engineers of the electronic recording systems.

This solution has been beneficial as it offers technical accuracy, is low cost, and allows efficient and effective management of controls and audits.

Belgium

In 2014, Belgium introduced legislation for certified cash registers, designed to address VAT fraud.

The solution consists of four important pillars: technical solution that secures data (making tempering detectable); certification of the devices; registration of all devices by the different stakeholders with the Ministry of Finance; and auditing on the field.

Technical features: The 'Registered Cash Register System' (RCRS) applies for the hospitality sector. This RCRS always includes three 'devices':

1. the Electronic Cash Register / Point of Sale (ECR/POS) with regulation specifying the forbidden and mandatory functions;
2. the Fiscal Data Module (FDM) that stores the relevant data;
3. the VAT Signing Card (VSC) that contains two certificates to digitally sign the receipt.

When a transaction is registered in the ECR/POS, the relevant content is transmitted to the FDM, where it is time stamped and stored and receives the digital signature. The data includes updated counters from the VSC. Some of the control data is also printed on the receipt, making signature verification possible. The digital encryption and signature is very strong, since the Public Key Infrastructure pair of keys is individually created by Belgium's certification authorities in a safe Hardware Security Module environment which is unknown to all other involved stakeholders (such as manufacturers of ECR/POS and FDM and taxpayers).

Implementation: Both the ECR/POS and FDM are available on the market, but each model must be certified by the Belgian Ministry of Finance's fiscal department.

In addition to the certification, Belgium introduced a registration system. This allows the Belgian Ministry of Finance to know exactly which taxpayers have what equipment, where it is installed and from what time. Furthermore, each certified software has to be hashed, which enables the Ministry of Finance to determine whether the installed system is a correct clone of the certified model or not. The fiscal auditors will have an audit tool to both analyse the FDM data and check the integrity of the data through automatic verification of signatures.

The solution has been introduced in the hospitality sector. Originally this applied to establishments with sales turnover of which at least 10 % consisted of meals to be consumed in the premises. In future, the target group will be limited to the establishments with a sales turnover of meals to be consumed in the premises that exceeds EUR 25 000. Full implementation is ongoing and expected to be finished by the end of 2016.

Results: The initial results from comparing the declared sales turnover on meals in the restaurants that installed the solution during 2015 with the sales turnover in 2014 shows an increase in 8%. This is notwithstanding that 80% of the restaurants taken into account in the 2015 sales results had only been using the solution for two months. There is also some evidence to suggest a longer trend of increased sales turnover since 2010 of over 20% each year, possibly indicating a 'whitening process' even before the RCRS became mandatory.

Canada (Quebec)

In the province of Quebec, the tax authority developed a Sales Recording Module (SRM).

There are four aspects to this solution: (1) an obligation on the business to provide receipt; (2) the receipt has to be generated using the SRM; (3) inspection activities by the tax authority; and (4) a public awareness campaign.

The legislative basis for the implementation was a modification of the Act respecting the Québec sales tax (CQLR, chapter T-0.1) and the Regulation respecting the Québec sales tax (CQLR, chapter T-0.1, r.2) as well as an amendment to the Tax Administration Act (CQLR, chapter A-6.002) to provide, among other things, for the imposition of penalties.

Technical features: The SRM has three main functions. The SRM receives, registers and sends the transaction data from the point of sale / cash register to the receipt printer. The receipt produced by the SRM must notably contain the total amount of tax due from the transaction, the date and time of the invoice, information on the establishment providing restaurant services, a barcode and a unique digital signature which guarantees the authenticity of the document. The data generated by the SRM also results in the standardised creation of accounting records for all bars and restaurants, which is a significant administrative benefit for taxpayers. The SRM also produces sales summaries which can be sent to the tax authority on request.

The tax authority identifies the specifications required in the point of sale / cash register in order to be compatible with the SRM, lists a number of compatible systems that meet them and can also issue certificates of compliance where an existing system has been adapted.

Enforcement: Inspections are conducted through the use of hand held computers. Inspectors may attend a restaurant posing as an ordinary customer or in uniform identifying themselves and verify if a receipt is issued to them for the meal. The device can then read the barcode on the invoice. This validates the signature on the invoice and identifies whether the invoice was produced using the SRM. The inspector can retrieve information stored in the SRM by downloading it onto a USB key and compare the data from the SRM to the information otherwise reported by the taxpayer.

The public awareness campaign consisted of launching a multimedia ad campaign in order to promote the new measures, thus informing the general public that the operator of a restaurant or bar is required to provide them with an SRM-generated bill, among other things.

Implementation: The SRM was first implemented in the restaurant sector, as there was evidence of sales suppression in this industry. When implementation was launched, 33 000 SRMs were installed in 20 000 establishments. The provincial government subsidised the purchase and installation of SRMs for a temporary period.

Results: At 31 March 2016, CAD 1.2 billion (EUR 822 million) in taxes was recovered following the introduction of the SRM into the restaurant industry. Projections are that, by 2018-2019, this will cumulatively amount to CAD 2.1 billion (EUR 1.44 billion).

The SRM was then implemented in the bar sector as of 1 February 2016. At the time, tax losses were estimated at CAD 76 million (EUR 52 million) per year.

The future plans include upgrading the solution and implementing it in taxi driving businesses.

Finland

Based on the Finnish Government's Resolution on a National Strategy for Tackling the Shadow Economy and Economic Crime for 2016–2020, an Action Plan against the Shadow Economy and Economic Crime has been drawn up. The Action Plan is dated 7 June 2016 and comprises 20 projects, one of which is a study on the applicability of type-approved point-of-sale systems in Finland.

According to the project, the tax administration will prepare a study on the applicability of type approved point of sale systems in Finland. The study will take into account technical implementation, costs to the authorities and businesses as well as impact assessments. Views on the study will be requested from business representatives as well as from other stakeholders involved.

The purpose of type-approved point-of-sale systems is to ensure the recording of cash transactions, prevent the manipulation of data by encryption methods and other technical strategies, and ensure that the authorities performing supervision have access to data in standardised form.

Because of the global trend, the study will focus on 'online' point-of-sale systems. The study will be implemented by the end of 2018.

France

In order to fight against VAT fraud related to the use of fraudulent software, the Finance Bill for 2016 establishes the obligation for merchants and other professionals subject to VAT to use a secure and certified cash register system or accounting software.

As of 1 January 2018, the use of a secure system will have to be attested by a certificate issued by an accredited organisation or an attested by a certificate issued by the publisher.

In cases where there is no certification meeting the requirements, a penalty of EUR 7 500 per item of software will apply, and the offender will have to rectify the situation within 60 days.

It is anticipated that some merchants will be able to comply by updating their existing software, as part of a maintenance contract purchased when buying the software.

Germany

Ensuring that digital records cannot be changed requires the introduction of legal provisions as well as technical measures. For this reason, the new Act on the Protection of Digital Records from Manipulation was implemented (Federal Law Gazette 2016 I page 3152). The intention is that all taxpayers who use an electronic cash register (both cash registers and computer-based tills) will be required to protect the system by means of technical security features.

The measures consist of the following elements:

1. Mandatory use of technical security features in an electronic recording system.
2. Introduction of cash register inspections.
3. Sanctions against violations.

Technical security features: The technical features of electronic recording systems include that it must consist of a security module, a storage medium and a digital interface. The Federal Office for Information Security will specify and certify the technical requirements for each of these components. The electronic basic records must be recorded individually, completely, accurately, promptly, in consecutive order and in a way that they are unchangeable. They must be saved on a storage medium and kept available. These requirements will make it possible in the future for the direct subsequent verification of individual transactions to take place.

Germany (continued)	A Technical Ordinance on the Implementation of the Act on the Protection of Digital Records from Manipulation will describe the requirements for the logging of the individual electronic records. Pursuant to the ordinance, a new transaction must be recorded simultaneously as it occurs by the electronic recording system for every transaction or other operation. This means the data is recorded and stored in a uniform process by means of which the logged individual digital records cannot be manipulated after it has occurred. For this reason, each transaction must be assigned the time of the start of the operation, an unambiguous consecutive transaction number, the type of operation, the date of the operation, the operation's end time or the time when the operation was cancelled, and a check value. If a manipulation should nevertheless occur, this can be detected at any time by means of the transaction chain. ***Inspections:*** Furthermore, unannounced cash register inspections will take place, in order to ensure a significantly increased risk of detection for the taxpayer. Cash register inspections will be used to verify conformity with the law, in particular the correct use of the technical security features. An inspection can take place without advance notice and will take the form of a special process aimed at promptly reviewing the correctness of the cash register records and whether the cash register records have been correctly entered into the accounts. In this context it is worth mentioning the digital interface, which will enable the auditors from the revenue authorities to carry out the inspection more quickly, as well as the option of more easily recognising whether the registration of the basic records is complete by means of the issued receipts. ***Sanctions:*** If violations of the new obligations regarding the proper use of the technical security features are detected, then this can be punished as a tax-related administrative offence with a fine of up to EUR 25 000, irrespective of whether any loss of tax revenue has occurred. This is intended to achieve a general preventive deterrent effect. ***Costs:*** It is anticipated that this solution would mean one-off compliance costs for industry totalling approximately EUR 470 million for the procurement of new equipment and the conversion of existing equipment, plus annual ongoing compliance costs of approximately EUR 106 million, which comprises certification costs, personnel costs relating to helping with inspections and ongoing costs for maintenance and support. These estimates are based on the following calculations: • Estimated 2.1 million devices affected. • One-off procurement and installation costs of approximately EUR 224 per device (EUR 470 million in total for industry). This includes the procurement of new equipment (around EUR 193 per device, or EUR 405 million in total for industry) and the retrofitting of existing equipment (around EUR 11 per device, or EUR 22.5 million in total for industry). According to estimates, around 411 000 devices could be replaced and 1.7 million devices could be converted. The total cost also includes an additional amount of around EUR 8 per device (or EUR 17 million in total for industry) for the acquisition of the security module for the conversion plus around EUR 12 per device (or EUR 26 million for industry in total) in personnel costs for the conversion. • A time burden of an average of 30 minutes per company and cash register inspection would be placed on industry. This estimate takes into account that inspection per company can be of different intensity and length. Based on the expected audit rate of all companies, this results in annual personnel costs of around EUR 343 000. An amount of EUR 50 per device per year was estimated for the purposes of maintenance and support (*e.g.* updating the cash register software). This would result in total costs for industry of EUR 105 million per annum.

Ghana

Draft legislation is being considered which would make it mandatory for specifically listed categories of taxpayers to use a fiscal electronic device, including offences and sanctions for failure to do so. This was borne out of the work of a cross-agency committee, including the ministry of finance, tax authority, attorney-general's department and others to study the problem, the technical options, the feasibility of a solution and cost / benefit analysis, which then made a proposal to Cabinet for consideration.

Technical features: the device will be linked to a central point in the tax authority, meaning transactions will be transmitted to the tax authority in encrypted form in real time. The device is also expected to verify / detect input tax claims by taxpayers and possible rejection of fraudulent ones. It is further expected to generate several management reports.

Enforcement: The data provided to the tax authority will be used to generate risk analysis reports, which would identify unusual data to be used for compliance activities. Field audit staff will perform a benchmark study at the start of implementation, which would be used in future for compliance. This has been based on experience from some compliance work performed in the past where field auditors were stationed in businesses such as shops or offices over a period of time to record sales, and thereafter the taxpayers did not subsequently report lower sales to the tax authority.

Benefits and costs: The committee established to study the feasibility of introducing the device estimate conservatively that the introduction of the fiscal electronic device would increase revenue mobilisation by 20%. It is also expected significantly improve taxpayer's record keeping and bring a substantial amount of the informal sector into the tax net. It is also expected to reduce the cost of tax collection. For taxpayers, implementation of the fiscal electronic device is expected to reduce record keeping costs for taxpayers, reduce transaction errors, and assist with stock management and recording employee activity and performance. It is estimated that the fiscal electronic device will cost USD 800 – USD 1 500 (EUR 726 – USD 1 362). The government is considering ways to support taxpayers in bearing this cost.

Greece

New legislation is planned, which regulates the product evaluation and authorisation of point of sale machines, as well as the requirements for businesses to use approved point of sale machines.

Product evaluation and authorisation: In order to be an approved point of sales machine, it must meet the required technical specifications. This device must contain a port for sending its identification data online to the server of the tax authority. If approved, it is authorised for sale in the Greek market, known as a Fiscal Electronic Device.

The process for approving a point of sales product is as follows. Every manufacturer or importer of such machines must seek approval from a committee in the Department of Fiscal Electronic Cash Registers and Systems which is part of the Ministry of Finance. The application includes submission of a working sample of the fiscal model for evaluation and test.

The committee is responsible for checking whether the machine meets the technical specifications, in conjunction with expert evaluators in the National Technical University of Athens.

Once a model has successfully passed all tests, the committee issues the applicant with a unique license number for the specific model. This license number is included on each receipt and affixed on the approved model. This enables any person to check the lawfulness of a specific model by looking at the license number on the issued receipt.

Greece (continued)	***Requirement for businesses:*** A business selling goods and services in return for cash payments must have a Fiscal Electronic Device. Whichever device is used, the taxpayer is obliged to print a receipt for each retail transaction and give it to the customer. Only receipts issued by an approved model of Fiscal Electronic Device are considered as official, legal receipts (see also information on electronic invoicing below). Exemptions may apply in the Decision of the General Secretary of Public Revenue (1002/31.12.2014). The taxpayer must keep a copy of each receipt in either a hard copy or electronic journal. If kept in an electronic journal, this must also be signed at the end of each day. At the end of each day, a report must be printed with the daily totals. These must be kept for at least five years and must be presented to auditing authorities on request. The daily report is verified as authentic through the use of a signature. The signature is created upon final issue of the daily report and is registered as a special record in the device memory, accompanied by the date and time and printed on a special daily record signature slip. This slip is issued automatically without requiring the intervention of the operator of the device. It is then stored electronically. The device memory is protected in a special box, which is an integral part of the fiscal electronic device and is sealed with a special material such that the removal of the memory is impossible without destroying the cover of the device. The preservation of this data is independent of any integrated or external power source. The memory is either built-in and sealed inside of the device or installed as an external add-on. All receipts issued by the Fiscal Electronic Device during the day from the issue of the previous daily total report until the issue of the next daily total report are registered in an electronic journal. Consideration is being given to constructing a mechanism for the data with the digital signature for the transactions to be automatically transmitted to the tax authority server. The transmission of this data is encrypted and after the decryption is only accessible by relevant personnel in the tax authority and by the owner of Fiscal Electronic Device. ***Enforcement:*** These solutions are monitored and enforces as follows: • Legislation and regulations state that businesses providing goods or services to retail customers are obliged to inform customers of their obligation to issue receipts. Taxpayers may only claim a tax deduction with respect to the purchase if it can be verified with a legal receipt, giving them an incentive to ensure they obtain a receipt when they purchase goods. • Random audits will be undertaken by tax authorities to check that customers exiting the business have a legally issued receipt. • Strict penalties are imposed for a breach of the legal obligations, including for failure to maintain these records, distortion of fiscal devices, alteration of the data or destruction or corruption of these records.
Hungary	In 2014, Hungary introduced an online cash register. ***Technical specifications:*** Regulation includes technical specifications for the cash registers, the security requirements, the user identification process and rules on licensing cash registers. The data is recorded in a Fiscal Control Unit (FCU) equipped with a mechanical seal, which is embedded in the machine at the point of sales. ***Data transmission:*** The data is then transmitted in high frequency to the tax authority. Having regard to the need to ensure reliability, it was considered best to use mobile phone network operators as they are identifiable and reliable service providers, and the mobile network covers almost all of the country. To ensure confidentiality, bank-level cryptographic solutions have been introduced, the infrastructure of which is provided by the tax authority.

Hungary (continued)

Implementation: The IT-solution was developed by market players based on published criteria and a competitive tender from the market was launched. The system was first introduced in the retail and hospitality sectors which had previously been obliged to use (not on-line) cash registers as well, and in 2016 it was expanded to the service sector and to car dealerships and car parts dealers. More than 225 000 cash registers are connected to the system. In order to obtain the solution, small businesses receive subsidies for up to five changes of cash machines.

Inspection: The tax authority has mobile inspection devices, from which display operating cash registers on a map. Using these devices an inspector can directly access the data of a particular taxpayer. The incoming data are stored in a data warehouse which allows continuous risk assessment, analysis, and setting up a list of shops selected for spot checks. The auditor can also verify whether the number and type of electronic cash registers in a particular shop match the number and type registered in the central database, as well as check whether the amount of money or money equivalent in the cash register matches the amount recorded on the fiscal control unit.

Results: In the first year of introduction (2014), VAT revenue increased by 15% in the concerned sectors, and as a result, the increase in VAT revenues has exceeded the overall costs of the whole project already during the introduction. Since then, there has been a continuous clearing of the economy in the concerned sectors. In addition, there was an increase in the number of employees registered for tax.

Italy

To address the risk of data alteration using illegal sales suppression software, Italy introduced Legislative Decree no. 127 dated 05.08.2015. The Decree is designed to encourage the electronic transmission of payment data as well as the use of e-invoicing (electronic documents undersigned with electronic signature). See below for more detail on electronic invoicing.

It applies to retailers, and introduces a cash register system directly transmitting data to the tax authority at the end of each day, securely and without altering any information. In this way, some accounting obligations are not due.

This measure is designed to:

- Boost the risk analysis.
- Simplify the system.
- Promote and support the digitalisation.

Kenya

Kenya is currently testing a new solution, Accounting Command Language, I Tax Management and electronic cash registers to address the problem of manipulation of sales data, and non-reporting of sales transactions. These are focussed on the risks posed in the construction sector, supermarkets and shopping malls and medium – large taxpayers.

Additional tax has been reported since tax transactions have been required to be performed online such as tax return filling and payments. Audit and investigation modules are at an advanced stage of being implemented.

Netherlands

In the Netherlands a “voluntary” quality-mark is developed.

Features: A cash register with a quality mark fulfils the requirements to store and process data reliably, and whereby alternations to transactions can be detected. The set of quality mark indicators were developed with inputs from many developers and distributors of cash registers.

Implementation: The Netherlands Tax and Customs Administration encourages the implementation of these “quality-mark” point of sale-systems in the whole market. In particular, it focussed on franchisors, which have an interest in preventing any harm to the name and reputation of their business. The tax administration made an agreement with the franchisees on checking doubtful returns based on EDP scripts. Any improbabilities were shared with the franchisor and they were given the opportunity to explain the findings.

Netherlands (continued)	***Results:*** The results of this were positive. Of 45% of the fraudulent franchisees, 85% came to a voluntary agreement with the tax administration in order to restore the misconduct. The profit from investigated supermarkets alone was around EUR 15 million, including fraud cases and voluntary statements of franchisees. The publicity may have also had an impact on these results. Another aim was to establish a change in behaviour among franchises by creating an atmosphere in which committing fraud was unacceptable. The has led to more governance in the sector, more control mechanisms like new software tools, more transparency between retail organisations and more discussion between supermarkets about audit mechanisms and experiences.
 **Rwanda**	Rwanda has introduced legislation and regulations requiring Value Added Tax (VAT) registered taxpayers to buy and use and electronic billing machines (EBM). ***Context of introduction of EBM:*** • Manual invoicing systems were paper based which are easily destroyable by fire, water or any other disaster. • Forgery of invoices resulting into unreported sales and undue VAT refund claims. • Double sales invoice books (especial large, medium or small family owned businesses). • Cost and time taken during tax audits. • Lack of transparency in the course of tax audits. ***Legal framework:*** Law No 37/2012 Establishing Value Added Tax as modified and complemented to date and Ministerial Order N° 002/13/10/TC of 31/07/2013 on Modalities of Use of Certified Electronic Billing Machine. For reference, the Ministerial Order is available here: www.rra.gov.rw/typo3conf/ext/complete/Resources/Public//download/pdf/ogazette.pdf ***Technical features:*** There are two aspects of the system: a Certified Invoicing System (CIS) and a Sales Data Controller (SDC), also available certified All in One device incorporating CIS and SDC features in one device and certified software meeting CIS requirements. The CIS is the point of sale machine, which must send the transaction data to the SDC. Each CIS has a unique registration number. The CIS must generate a receipt containing at least the following data: taxpayer's name; identification number; address where the sale took place; receipt type and transaction type; serial number of the receipt in uninterrupted ascending number series; description of the sale / service items with quantity, price and other actions such as cancellation or corrections; total sale amount; tax rate; tax on the sale; means of payment; SDC information including date and time stamp, sequential receipt number, receipt signature and SDC identification number; data and time stamp by CIS; machine registration code. The SDC is connected to the CIS and processes and stores the receipts. The SDC is secure and tamper-proof, and each certified SDC has a unique serial number. The SDC assigns an electronic signature to the transaction which is printed on the receipt. The signature is verifiable by the tax authority using a special decryption tool which is unique for every installed SDC device, meaning that falsification of the signature can be immediately detected. The electronic billing machine must be clearly visible to customers, with a statement including the name of the user, the unique identification numbers for the CIS and SDC, and that customers should not pay if a receipt is not issued. The electronic billing machine must be connected to the tax authority's server accessible to both the customs and domestic tax officials. Data is transmitted in encrypted form. The tax authority can then perform local audit or remote audit.

Rwanda (continued)

Implementation: Implementation of the electronic billing machine requirements is occurring in a progressive manner, with the tax authority specifying particular categories of taxpayers required to use electronic billing machines. Once fully implemented, every business registered for VAT will have to provide a customer with a special receipt issued through the electronic billing machine for every sold good or service.

The suppliers of electronic billing machines must obtain authorisation from the tax authority in order to obtain certification of their systems. This includes a test of the software through a live demonstration or machine inspection. Once certified, the supplier is added to the list of certified products which is published on the tax authority's website. Taxpayers will either procure the electronic billing machine from the list of certified suppliers, or if they choose to modify their existing system, this must be specifically inspected and authorised by the tax authority as meeting the requirements.

Benefits of EBM for taxpayers:

- EBM constitutes an internal control tool.
- EBM helps in stock taking.
- EBM data serve for accounting purposes.
- Information safely kept.
- A means for business transparency.
- A means of information for business stakeholders and partners.
- Less time and financial audit costing.

Benefits of EBM for the tax authority

- Real time sharing of information between tax administration and taxpayers.
- Information safely kept.
- Less time and financial audit costing.
- Improve transparency in tax audit process.
- Improve the VAT refund process.
- Improve the level of VAT collections.
- EBM constitutes a management tool and an efficiency control mechanism.

Results: In March 2013, implementation started with 800 machines. At July 2016, there are now 13 520 machines which are used by 85% of the VAT registered taxpayers. VAT collections have increased since the introduction of EBM:

- In March 2013 to June 2014, EBM contributed to the increase of 6.5% of VAT collections.
- VAT collected on sales increased in 2015 by 20% when compared to 2014.
- VAT payable registered an increase of 22% for 2015/2016 fiscal year compared to 2014/2015 fiscal year.
- Cases of undue refund claims identified and prosecuted.

Rwanda (continued)

Implementation challenges:

- Low culture of invoice requesting whenever a sale is made.
- EBM users not issuing EBM invoices (they issue manual invoices, delivery notes or simply nothing) especially in service industry such as in Restaurants, Bars but also in Supermarkets.
- EBM users issue an invoice with the price lower than the actual money received.
- Misuse of tax rates (taxable goods considered as exempted ones).

Enforcement: Each taxpayer that is required to use an electronic billing machine must register with the tax authority. The tax authority has the power to conduct inspections of electronic billing machines to verify compliance with the technical specifications and other taxpayer obligations with respect to the electronic billing machine. Substantial fines will apply to businesses that do not install and use the electronic billing machine as required, and to suppliers of CIS or SDC machines.

The tax authority has also used enforcement and deterrence strategies including the following:

- Education and sensitisation of consumers.
- Sensitisation of university, secondary schools students, religious leaders, private and public institutions.
- Consumer motivation "EBM lottery scheme".
- Introduction of Supply Chain Management software.
- Mystery shopping.
- Understanding of price structure for some commodities.

More information is available here: www.rra.gov.rw/index.php?id=33.

Slovak Republic

Electronic cash registers were introduced in the Slovak Republic in 2008. The legislation with effect from 1 January 2015 extended the list of service providers who must use electronic cash registers ("ECR") when selling goods and services and also created a virtual electronic cash register ("VECR").

Technical features: The VECR is a platform set up on the Financial Directorate's website and communicates with devices such as PC, tablet or smartphone and a printer. The Financial Directorate developed the VECR application and made it available free of charge for all the entrepreneurs that are obliged to use cash registers.

Compared to a receipt issued by the ECR, the receipt issued by the VECR contains a unique identification code and QR code with all the data of issued receipt but also identification data about the entrepreneur: business name of entrepreneur, billing address, address of the sales point, tax identification number, and VAT identification number.

Access for the tax administration: All the financial transactions made by the seller are saved on the Financial Directorate's servers and are accessible to the tax administration. Tax auditors can immediately access information about all the users such as the location of the sales points, the issued receipts (fiscal receipts), the other receipts (non-fiscal receipts), the amount of money in the VECR´s cash drawer and they can generate financial closing accounts or reports including financial data regarding to a specific VECR user and a specific time interval.

All the reports generated by the tax auditors are easily processable with analytical software like IDEA from their desk. Tax auditors can run analytical tests over the reports and can gain exact knowledge about the entrepreneur's fiscal behaviour and detect risky fiscal transactions (e.g. issuing lots of non-fiscal receipts, issuing receipts with returned items which are reducing the tax duty). Using the data from VECR and analytical tools such as IDEA can contribute to a more effective selection of sellers for later auditing.

Slovak Republic (continued)

Third party verification: The QR code can be easily checked by another application developed by the Financial Directorate named "Check the receipt", an application designed for the customers or clients so they can verify themselves the data contained in the receipt issued with the VECR. If customers or clients find that the data on the issued receipt does not match the data on the VECR server, they can contact the Financial administration.

Next steps: The Financial Directorate is working on another application which will be used by the tax auditors on the premises where the tax audit takes place. This new application will be connected to the VECR server and will provide tax auditors with on-line and on site information about the fiscal behaviour of the entrepreneurs, the issued receipts and allow them to generate financial closing reports.

This new application should help the tax auditors to audit and control service providers even more efficiently.

Sweden

Sweden requires that sales must be registered in a cash register connected to a fiscal control unit.

Technical features: The cash register must meet a certain standard, which the manufacturers of the cash register are responsible for meeting. The fiscal control unit must be certified by a specific body in the Swedish tax authority. Taxpayers must register with the tax authority to confirm that they are using a cash register connected to a fiscal control unit.

The requirements for the content of the data that must be recorded in the fiscal control unit are included in regulations. This includes:

- One log for counters: The total number of receipts issued, missing receipts, the number of regular receipts, the number of training receipts, the number of copies of receipts, the total sales and the grand total.
- Another log for specific information about each receipt: receipt number, date, time, sales amount, VAT amount, and a unique control code generated by the control unit.

The information in the control unit is encrypted and can only be read and decrypted by the Swedish tax authority.

Implementation: Sweden targeted all sectors that are selling goods and services which are often paid in cash. Some general exemptions apply, including for taxis, e-commerce, vending machines, amusements games, slot machines, and governmental or municipal organisations. It is also possible for taxpayers to apply for an exemption, where the bookkeeping is reliable and that the fiscal control can be guaranteed in other ways than using a control unit; or if it is unreasonable for any reasons to have a certified cash register. The cost for implementation was in average about EUR 2 500 per cash register, including hardware and installations costs.

Enforcement: The tax authority analyses information from the electronic journal and from the control unit using traditional e-audit methods. In addition, the tax authority conducts a lot of unannounced on sight inspections to verify whether receipts are given and that sales are registered, as well as doing undercover purchases posing as customers and counting customers. Penalties can be issued if a sale is not registered. The information from the inspections is then used as feedback to determine risk levels for follow up action. The visibility of enforcement actions has been crucial for acceptance of the legislation and compliance, as well as ensuring a level playing field between businesses.

Results: Compliance has increased both among users of cash registers and the manufacturers of cash registers. Manufacturers are more compliant and the tax authority has not found any zappers or phantomware since the legislation was implemented.

The immediate revenue effect once the requirements were introduced was a 5% increase in the reported revenues. The estimation of the ongoing effect will be at least a 1% increase in reported revenue. This means that the reform has resulted in increased tax revenues of at least SEK 3 billion (EUR 320 million) per annum as a result of reduced tax evasion. In addition, the introduction of the fiscal control unit has had a significant preventative effect which has also contributed to increased revenue collection.

Annex B

Catalogue of country solutions for electronic invoicing

Argentina • Greece • Italy • Kenya • Mexico • The People's Republic of China • Singapore • Slovak Republic

Annex B

Catalogue of country solutions for electronic invoicing

Argentina

Argentina has used mandatory electronic invoicing for certain sectors since 2007 (and optional electronic invoicing since 2006). Since then, the use of the electronic invoices has been expanded in a gradual and phased manner according to the business activity and type of taxpayer. During 2016, the implementation will be completed so that it will be mandatory for all taxpayers registered for Value Added Tax (VAT).

Technical features: The model is based on the "online" authorisation of the documents. This means that the taxpayer, after the approval of the operation, has to apply to the tax authority for authorisation so that the document is considered an invoice and has fiscal effects against third parties. The information is validated online and if the invoice is authorised it is given an authorisation code and all the information entered is kept in the database of the tax authority. In this way, the revenue body has the information of the issuer and receiver of the invoice, of the applicable tax debit and the possible tax credit to compute before the submission of the VAT return.

For more details see General Resolution N° 2485/08 AFIP www.infoleg.gov.ar and www.afip.gob.ar/fe/#que.

Benefits: The implementation of digital documents has had the following advantages and strengths (also relevant for electronic sales suppression above):

- There is a formal control at the moment of authorising the printing of receipts.
- The tax authority has timely access to the tax debit and possible calculation of tax credit of the transactions.
- The digitalisation of the information, together with technological developments, allow for the exploitation of large volumes of data more dynamically.
- They place the obligation on the taxpayer to comply with the procedures and include the data in the making of the receipts in accordance with the existing rules, reducing the administrative cost for the tax authority.
- Once the transaction is registered, the possibility of it being subsequently falsified is significantly reduced as the invalidation of a receipt may only take place with a new document adjusting the previous one, leaving a record of the change, or through a fraudulent manoeuvre that violates security standards in the electronic cash register.
- There is an increased risk perception on the part of business and customers because the information in electronic format and there are tools for third parties to verify receipts.

Enforcement: Electronic invoicing is monitored and enforced as follows.

- There is a tool designed to verify receipts, whereby the receiver of the electronic invoice, or entities dealing with tax/social security procedures, are able to verify if the information contained in the receipt matches the information timely entered and authorised by the tax authority. The online authorisation model provides an almost immediate response to taxpayers has proved to be very productive from its early stages in 2006 and has assisted progress with the generalised implementation of the electronic invoice system to more sectors and taxpayers.
- The information on invoices received through the authorisation process provides valuable information to perform cross-checking with other data recorded by the tax authority.

- Publication on the web site of a list of non-reliable taxpayers, based on the controls performed. The consequence of publication is limitation on the use of the individual Taxpayer Identification Number and temporary suspension of the authorisations to issue invoices.
- The solutions implemented strengthen the controls performed by the tax office and in turn generate risk perception by the taxpayers.
- In addition, although many of the measures are preventive, ongoing control is required to maintain the risk perception levels. It is also necessary to periodically define new prevention tools to respond to emerging risks and technologies.

Results: The results and impacts of the incorporation of the electronic invoice in Argentina have generated positive effects in a gradual, phased manner, together with the progress of its implementation during the last 10 years. To date, there are more than 750 000 users already incorporated in the system and more than 4 billion electronic receipts have been issued.

Greece

Greece is in the process of introducing electronic invoicing requirements.

Technical features: All invoices, credit notes and consignment notes issued by computers will be required to be signed electronically using a special licensed fiscal electronic signature device (FESD). Each relevant business will be required to buy an approved FESD or adapt the existing computer equipment to meet the technical specifications. This is one of the methods of authentication under the L.4308/2014.

When the invoice is printed, the unique e-signature generated by the FESD is printed at the end of the document. This works as follows. After entering and formatting the data to be printed in the computer, and after initialisation of the record issuing – printing, the computer's software saves, communicates and transmits to the FESD the set of the required data of the slip being issued. The FESD receives this data, processes it with a special security algorithm (SHA-1) that creates a hash value (sign) and sends the result of this processing back to the connected computer. The hash value, which represents a sequence of characters and digits, is the unique electronic digital "fingerprint" of the data of the slip being issued. The FESD saves this hash value into his own working daily memory and issues a relevant slip – receipt with the date, the time, the daily ascending sequential number and the general ascending sequential number of slip issue.

All the produced signatures are stored securely the inside FESD's memory at the end of each day and collated in a day-end report. The day-end summary report is also assigned a unique e-signature and saved permanently in the secure fiscal memory of the FESD. These must be preserved for at least five years and provided to tax auditors in an audit. These files are considered as primary transactional data and must be reflected to the totals in accounting books.

Each day the business owner automatically sends the summary file to the tax authority server, in encrypted form to be decrypted automatically only by the server. The fiscal data are accessible by the owner of FESD and by the authorised personnel of the tax authority.

Benefits: The validity and integrity of those files are checked using an algorithm. It takes approximately two minutes to check 150 000 invoices stored on a CD, running an application on a typical laptop.

Italy

Italy first introduced an obligation from early 2014 for electronic invoicing for the supplies to the public sector. Electronic invoices are the only type of invoice that will be accepted by the public sector bodies procuring supplies.

Technical features: The supplier must use the transmission channel identified by the tax authority (the Exchange System) for transmitting the invoices to the tax authority. The electronic invoicing has the following characteristics:

- The content is structured in an XML (eXtensible Markup Language) file. This format is the only one accepted by the Exchange System.
- The authenticity of origin and the integrity of the content are guaranteed by the person who issues the invoice by affixing a certified electronic signature or a digital signature.
- The transmission is conditional on the presence of the unique identification code of the office to which the invoice is addressed, and which can be found in the Index of Public Administrations.

Expanded implementation: Electronic invoicing is now being expanded for use in transactions between private businesses. Legislative Decree no. 127 of 5 August 2015 introduced measures for the electronic transmission of data on VAT transactions to the Revenue Agency. For transactions carried out as from 1 January 2017, taxpayers that supply goods and retail services (pursuant to Article 22 of Presidential Decree no. 633 dated 26.10.1972) may choose between:

- Supplying information to the Revenue Agency in a more manual fashion, including customers and suppliers lists, black list transactions, summary statements for intra-EU acquisitions of goods and services; or
- Transmitting electronically to the Revenue Agency all the invoices issued and received without any other communication obligations.

The tax authority is making software available to businesses for free from July 2016 to conduct electronic invoicing in business to business transactions enable the operators (especially the micro-small enterprises) to issue, transmit and store the electronic invoices.

Results: In the first implementation period of June 2014 – February 2015, 2 672 780 invoices were received. The tax authority is enhancing the processes to cross-check data, such as domestic supplier and customer listings which allow crosschecking of data submitted by domestic suppliers and customers so that potential tax gaps and losses can be intercepted. The electronic storage and linked transmission of the payment data will replace the obligation of fiscal certifications of the payments through the issuance of fiscal or cash register receipts.

The widespread adoption of the electronic invoicing and data transmission tools, besides resulting in substantial reductions of the compliance procedures for taxpayers, will greatly enhance the detection and prevention of tax evasion, since the information available to the tax authority will allow it to carry out more precise risk analyses, through the execution of verifications and data cross-checks in an automatic and timely manner.

Kenya

Kenya is using Accounting Command Language to manipulate data and to check repeated invoices and skipped invoices. The focus is on all taxpayers, but medium – large taxpayers in particular. Although there have been some initial challenges in using the tool, the results have shown that where it is used regularly, the result has been very positive.

Mexico

Mexico introduced electronic invoicing in several stages.

Prior to its introduction, taxpayers used only printed invoices, which were freely prepared and printed without tax administration controls. The disadvantages were that there was a high volume of false transactions using fake invoices to claim tax deductions and reduce tax; a high volume of hidden income in cases where no invoice was issued; and compliance action by the tax authority required manual checking.

Mexico (continued)

The first stage: Establishing controls

A requirement was introduced such that only authorised printers could produce invoices. All invoices were required to have a unique number which was controlled by the tax authorities and the authorised invoice number had to be linked to an updated taxpayer register. The printer produced reports of the invoice numbers that were issued.

The results of this stage indicated that the authorised printers increased taxpayers' perceptions of risk. However, a black market of "cloned" invoices emerged which were produced by the authorised printers. A cloned invoice had a real folio number, but contained false amounts and false clients. Because of this, the tax authority could not check the operations of all authorised printers.

The second stage: from 1990s

The tax authority focussed on making intensive use of new technologies. This included the use of digital advanced signatures; internet services; standardised electronic documents; and enhanced data analysis.

The result: this led to the creation of the first electronic invoice (e-invoice), referred to as "CFD".

Third stage: from 2005

The standardised e-invoice contained the folio number which was controlled by the tax authority as well as the taxpayer's digital seal. The tax authority received monthly folio reports. The e-invoices used XML (eXtensible Markup Language) tags, as it ensured easier electronic data exchange and thus allowed compliance with the technological standard to be an automated process.

At first, the use of e-invoices was optional for taxpayers. The use of e-invoices was then made mandatory for larger corporations. The taxpayer either devised their own systems to create the e-invoice or used the services of a provider.

The result: the number of false invoices was reduced. Larger taxpayers took advantage of the standardised electronic XML documents in their broader record keeping and administrative process and pushed their providers to use e-invoices. Technology companies started developing software to use and manage data from e-invoices.

Some problems remained. Some issuers did not comply with the obligation to submit monthly folio reports to the tax authority. The implementation cost was an obstacle for adopting the e-invoice for some taxpayers and some taxpayers preferred to continue using printer invoices.

Fourth stage: enhancing the e-invoices from 2011

Enhancements were made in order to ensure the best data use of e-invoices and make their issuance by taxpayers easier. E-invoicing would work as follows. This resulted in a 134% increase in the number of e-invoices issued from 2010 to 2011.

Step 1: The customer requests a fiscal receipt from the vendor, who generates the e-invoice and digitally stamps it according to the standards.

Step 2: The vendor sends the e-invoice to an Authorized Certification Service Provider (PAC). The PAC is a trusted third party authorised by the tax authority.

Step 3: The PAC validates the structure, syntax and tax attributes of the e-invoice. If it is valid, the PAC digitally stamps it with the folio number on behalf of the tax authority. The folio numbers were assigned online by the tax authority to the authorised certification service providers. The PAC also sends a copy of all invoices to the tax authority in real time in XML format.

Step 4: The PAC returns the validated e-invoice to the vendor, who then sends it to its customer by converting it from XML to PDF format.

Step 5: Both the customer and vendor can verify the authenticity of e-invoices.

Mexico (continued)	***Results:*** The only kind of invoice in Mexico is now e-invoice by internet. The use of e-invoicing has been expanded for use in payroll. A similar format and standardisation is also being used to document withholding tax and payments for dividends, trust operations, derivatives, payments abroad and electronic accounting reports. As at September 2014, there were 3 837 876 issuers of electronic invoices, and since introduction almost 13.5 billion e-invoices had been issued. Mandatory electronic invoicing in Mexico brought 4.2 million micro businesses into the formal economy.
 **The People's Republic of China**	In 2003, the VAT anti-counterfeit tax control system was introduced throughout China, covering all the general taxpayers. In 2014, the VAT invoice processing system was upgraded, and was rolled out step by step by the State Administration of Taxation of China (SAT) from 1 Jan 2015, applicable to both general taxpayers and small scaled taxpayers above a de minimus threshold. ***Technical features:*** The new VAT invoice processing system boasts of collecting comprehensive VAT invoice data, including name of taxpayers, name and code of goods (services), price, quantity, tax base, tax rate and amount of tax payable, etc. Taxpayers upload the encrypted VAT invoice data into the database of tax administrations via internet, each invoice with a digitally signed certificate. The invoice data is transmitted in a real-time fashion fully monitored by tax administrations, and then classified and sent to receiver taxpayers as the basis of tax filing, verification of the invoice authenticity, revenue source management as well as data analysis and utilisation. ***Benefits:*** When a taxpayer files a tax return, the new VAT invoice processing system will automatically cross-check the data of both input tax and output tax against those in the invoice database of tax administrations to prevent against under-reporting of the tax payable or over claim of the input tax. Moreover, combining the VAT invoice data with the tax return information, tax administrations across the country can also conduct tax risk analysis and economy-taxation correlation analysis, with a view to detecting potential tax risks and providing inputs for economic decision-making. To sum up, with a broad prospect of application, the electronic data of VAT invoices will play a positive role in standardising tax administration, preventing and controlling tax risks, and conducting economic performance analysis.
 **Singapore**	Singapore has implemented a cross referencing system to detect incorrect Goods and Services Tax (GST) information. ***Technical features:*** This system captures sales and purchase transaction listings which are requested from GST taxpayers through routine audits. The listing of information provided is determined by the scope of the audit and would be complete in relation to the scope of the audit. A standard data format is prescribed by the tax authority for taxpayers under audit to submit sales and purchase listings. The standard format is in Microsoft Excel. ***Benefits:*** These transactions are then cross referenced with transactions submitted in the past to uncover discrepancies. There are three main purposes for the cross-referencing system: • For the tax authority to match transactions in the sales / purchase listings obtained from the audited taxpayer against any existing transactions listings in the database (using the same supplier/customer ID and invoice number); • For the tax authority to carry out third party confirmation for selected transactions that are "unmatched" in the database to verify if the claims are in order; • For the tax authority to identify the network of entities that have substantial transactions with each other and the flow of such transactions - particularly in suspected fraud cases - to all GST taxpayers across all industries.

Singapore (continued)

The data is uploaded into a database system. The system will then enable auditors to cross reference transactions which have been submitted previously to uncover discrepancies. Periodically, certain transactions will also be selected to be sent to the businesses' suppliers and customers for third party confirmation.

Results: The main strength is to maximise the benefits of existing audit processes by making available collected data for use in future audit cases. In addition, the tax authority's compliance strategy subjects high risk industries and taxpayers to more frequent audits – hence, the system will have more transaction data for high risks taxpayers.

Challenges: The main weakness of the system is that it does not have full coverage of transactions, as data submission is triggered only when an audit is carried out. The tax authority may, in the future, consider exploring e invoicing with 100% coverage of GST taxpayers.

Slovak Republic

In the Slovak Republic, the VAT control statement (domestic recapitulative statement) came into effect on 1 January 2014. It was implemented by Amendment § 78a Act No. 222/2004 Coll. on value added tax.

Technical features: The VAT control statement is provided by both the supplier and the purchaser, and is provided to the Financial Administration electronically in XML format. Data is provided monthly or quarterly (according to the taxable period, with the latest due date being the same date as submission of the VAT return. The VAT control statement contains all types of transactions (input supplies, output supplies, and electronic cash register receipts). Each transaction in the VAT control statement is identified by VAT number of the supplier and the VAT number of purchaser, with the number of the invoice, date and value.

Benefits: Automatic cross-checking of data provided by the supplier and the purchaser in the VAT control statements (and combined with information from other sources on risk factors) allows us to detect:

- carousel fraud and chain fraud;
- issued invoices that later on are not recorded in the accounting;
- varying of accounting;
- replacement of invoices in the accounting;
- not-issued invoices;
- not using electronic cash registers;
- non-taxable persons issuing the invoice with tax included;
- taxable persons that applied twice for tax deduction from the same invoice in two different taxable periods.

Results: During the years 2014 and 2015, amount of risky VAT detected in domestic chain frauds was more than EUR 500 million.

- Effective planning of tax audit and performance – elimination of a human factor failure in auditing taxpayers, exactly specified set of questions derived from the retrieved data and its evaluation, when dealing with tax audit.
- Encouragement of voluntary compliance.
- Early awareness on tax fraud, its new trends and the territorial determination.

Bibliography

OECD (2013), *Electronic Sales Suppression: A threat to tax revenues*, OECD Publishing, Paris, www.oecd.org/ctp/crime/electronicsalessuppressionathreattotaxrevenues.htm

PriceWaterhouseCoopers (2015), *The Sharing Economy*, www.pwc.com/us/en/technology/publications/assets/pwc-consumer-intelligence-series-the-sharing-economy.pdf (accessed on 1 March 2017)

European Commission (2012), *Study to quantify and analyse the VAT Gap in the EU 27 Member States, Final Report, TAXUD/2012/DE/316*

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

For more information:

ctp.contact@oecd.org

www.oecd.org/tax/crime
@OECDtax

OECD
BETTER POLICIES FOR BETTER LIVES