A HOOVER INSTITUTION ESSAY

Buying Data and the Fourth Amendment

ORIN S. KERR

Aegis Series Paper No. 2109

In *Carpenter v. United States*,[1] the Supreme Court held that the Fourth Amendment requires the government to obtain a warrant before compelling a cell phone service provider to disclose at least seven days of a user's historical cell-site location records. This is a groundbreaking holding. For the first time, users have Fourth Amendment rights in corporate records about them that they did not make, cannot control, and likely do not even know exist.

Carpenter prompts a question: If the Fourth Amendment requires a warrant for the government to *compel* a provider to hand over records, is the same true if the government *buys* those records instead?[2] Put another way, if the company is willing to sell the records to the government—or has already sold them to someone else who will sell them to the government—can the government purchase the records without a warrant as an end run around *Carpenter*?

This essay offers two responses. First, existing law leads to a clear answer: The government can buy business records without a warrant or any cause. The Fourth Amendment does not apply. The reason is that a company will have common authority over business records that it has created and controls. That common authority permits third-party consent. When a company voluntarily sells its business records, its consent renders any search of the records reasonable. Although sales of user communications contents might present a different case,[3] the sale of noncontent business records—what I call "*Carpenter*-protected records," as they are business records protected because of *Carpenter*—is permitted. As a matter of Fourth Amendment law, the company can do what it wants with its records even if users with Fourth Amendment rights oppose it.[4]

The second response is a caveat to the first. Although current doctrine gives a green light to buying *Carpenter*-protected records, a sea change in how often the government can buy records to conduct detailed surveillance might someday justify a more restrictive approach. This possibility is based on the equilibrium-adjustment principles driving *Carpenter*. When new technology and social practice threaten to create a privacy dystopia, the argument goes, Fourth Amendment rules may have to be tweaked to restore the traditional balance of government power. This possibility should be more theoretical than real, however, for buying *Carpenter*-protected data. Based on the public record, the factual basis does not exist

for an additional adjustment. Buying records has not become a substitute for the detailed surveillance *Carpenter* addressed. In my view, meeting the high bar of equilibrium-adjustment would require a seismic shift in government power that has not emerged. For the foreseeable future, the Fourth Amendment law of buying *Carpenter*-protected databases should be simple. It is allowed.

This essay develops its argument in three parts. Section 1 considers the law of buying records before *Carpenter*, focusing on what I call the "willing seller" rule. Section 2 argues that *Carpenter* does not alter the willing seller rule because third-party consent permits the sale of *Carpenter*-protected records. Section 3 considers the possibility that widespread purchases of records may justify a different result, concluding that it is a theoretical possibility but is not justified based on existing practices.

I. The Willing Seller Rule before *Carpenter*

Before *Carpenter*, the Fourth Amendment law of purchasing business records was straightforward. Under the third-party doctrine,[5] users had no Fourth Amendment rights in a company's business records. The only rights-holder was the company that possessed the records. If the company sold its records, that was up to the company. I will call this the "willing seller" rule, and it meant that a market in business records raised no Fourth Amendment issues.

The willing seller rule follows from the Supreme Court's decision in *Maryland v. Macon*.[6] Baxter Macon was a clerk at an adult bookstore. An undercover detective entered the bookstore, browsed for a few minutes, and then purchased two magazines from Macon using a marked $50 bill. The detective believed the magazines were obscene, so he later returned and arrested Macon and retrieved the marked bill from the cash register. Macon was charged with distributing obscene materials, with the key evidence being the magazines purchased from him by the detective. Macon moved to suppress the magazines as the fruit of an unreasonable search and seizure.

The Supreme Court held that no Fourth Amendment violation occurred. First, entering the store and "examining the wares"[7] offered for sale was not a search, as the store itself was "intentionally exposed to all who frequent the place of business."[8] Second, buying the magazines did not seize them because they were the product of a voluntary sale. Macon had "voluntarily transferred any possessory interest he may have had in the magazines to the purchaser upon the receipt of the funds."[9] The detective merely took "that which was intended as a necessary part of the exchange."[10] "An undercover officer does not violate the Fourth Amendment merely by accepting an offer to do business that is freely made to the public,"[11] the Court reasoned, and that was true even though the detective had a "subjective intent to retrieve the purchase money"[12] after concluding the magazines were obscene: "Objectively viewed, the transaction was a sale in the ordinary course of business."[13]

Macon can be generalized. If you assume a person with Fourth Amendment rights in an item, the person can sell the item without triggering Fourth Amendment oversight. Baxter Macon could sell the obscene magazines to an undercover officer, and the entry to get the magazine was not a search nor its taking away after purchase a seizure. A drug dealer can sell an informant his product, and the approach to the buyer and taking away following the sale is not a search or seizure. When the transfer is made, the Fourth Amendment rights go with it. A voluntary sale in the ordinary course of business relinquishes all Fourth Amendment rights in the item sold.

Before *Carpenter*, the willing seller rule made the Fourth Amendment law of buying databases easy. The database seller was like Macon, and the database was like the obscene magazines Macon sold. Because the subject of the records had no Fourth Amendment rights in the database under the third-party doctrine, no other Fourth Amendment interest counted. "Objectively viewed, the transaction was a sale in the ordinary course of business" and the database seller relinquished its Fourth Amendment rights in the database when the database was sold (or its rights in the accessed portion of it when access to it was sold). The issue was apparently never litigated, whether because the law was clear or because a corporate seller of customer records is unlikely to face prosecution following a deal. But either way, the Fourth Amendment issues were straightforward.

II. Why *Carpenter* Does Not Change the Willing Seller Rule: The Role of Third-Party Consent

Now add *Carpenter*. *Carpenter* establishes that, at least in some contexts, users can have Fourth Amendment rights in a company's third-party business records about them.[14] A company may generate records about how its customers used the company's service, and it may use those records for business purposes. Users may have no control over the company's use or storage of the records. They may have no idea that the records even exist. For the first time, *Carpenter* gives users Fourth Amendment rights over at least some kind of such data, such that compelling company-created data held by the company can be a "search" of *the user's* "person, houses, papers, or effects,"[15] not just the company's. The company holds the data, but now two entities have constitutional rights in it: the company and the user.

Does this make a difference to the willing seller rule? I don't think it does. The reason is that the willing seller rule does not hinge on the seller being the only entity with rights in the item sold. Fourth Amendment law has a well-established way to deal with adverse relationships among multiple rights-holders. When multiple parties have rights, the willing seller rule is limited and defined by the familiar doctrine of third-party consent. This doctrine indicates that, when multiple people have Fourth Amendment rights in property, any person with joint access or control of it generally has the legal authority to control government access to it.[16]

The basic idea, drawn from *United States v. Matlock*,[17] is that "mutual use of . . . property by persons generally having joint access or control for most purposes" gives any one person "the right to permit the inspection [of the property] in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched."[18] As a matter of doctrine, then, a person with common authority over a place or thing can consent to a search of that place or thing, even if another person with rights in that place or thing would oppose the search, as long as the objecting party is not actually present and objecting.[19]

Combining the willing seller rule and the third-party consent doctrine mostly answers how Fourth Amendment law applies to buying *Carpenter*-protected databases. A provider that has created *Carpenter*-protected records will at the very least have common authority over those records. The company will have generated the records and stored the records for its own purposes. It will control whether the records are stored and how they are used. In contrast, users may not know the records exist or have any legal way to control what happens to them or even find out what they say. In that setting, the provider has more than just the mutual use needed to provide third-party consent. It has something more like exclusive use. And this means that third-party consent is permitted.[20] Because the willing seller rule permits rights-holders to sell what they own without triggering the Fourth Amendment, the provider can sell that access just as legally as it can decide to give it away.

The historical cell-site location information (CSLI) records from *Carpenter* provide a helpful example. As *Carpenter* explains, CSLI is created by providers behind the scenes. Phones "continuously scan their environment looking for the best signal, which generally comes from the closest cell site."[21] The network connections generate the records for the provider: "Each time the phone connects to a cell site, it generates" the record of the connection that can reveal, to various degrees of precision, the phone's location.[22] This is all done by the provider and for the provider: "Wireless carriers collect and store CSLI for their own business purposes, including finding weak spots in their network."[23] The typical user will not know the records were generated or stored. Indeed, *Carpenter* itself notes the possibility of selling the data, albeit in a modified form: "Wireless carriers often sell aggregated location records to data brokers," the opinion notes, "without individual identifying information of the sort at issue here."[24] Although *Carpenter* ruled that users have Fourth Amendment rights in the records, requiring a warrant to force the provider to disclose them, the provider retains access and control over the records.

From this perspective, *Carpenter* does not raise novel issues for the willing seller rule. Fourth Amendment case law routinely deals with the problem of shared rights over property where interests between multiple rights-holders diverge. And that case law gives any person with mutual use the authority to grant consent to a law enforcement search. Granted, the government will need legal process if none of the rights-holders wishes to provide the government access. But if one party with common authority over the property wants to

allow the government access to reveal evidence about another party, while others do not, access is permitted by third-party consent. A company can sell *Carpenter*-protected records without Fourth Amendment oversight because it has the common authority over the records.

No case law yet exists on this precise question. But we can get a feel for the issue by looking at lower court case law on shared rights in the contents of computers and computer files. The most analogous case is probably *Walker v. Coffey*,[25] a recent Third Circuit case involving voluntary disclosure of work emails stored on an employer's server. The Pennsylvania Attorney General's Office (OAG) was investigating Carol Walker, who was an employee of Pennsylvania State University, for forgery and various computer crimes. OAG approached the university and asked it to voluntarily produce Walker's university emails. University employees requested some kind of legal process, and then announced themselves satisfied when the OAG produced a subpoena for the email account that turned out to be invalid. The university then turned over the emails to the investigators. Walker later sued the OAG for violating the Fourth Amendment by obtaining her emails without a warrant.

The Third Circuit ruled that the Fourth Amendment was not violated because the university "was a third party with common authority over Walker's emails and the independent ability to consent to a search."[26]

> There is no dispute that the emails in question were sent or received via Walker's work email address, as part of an email system controlled and operated by Penn State. Thus, for purposes of the Fourth Amendment, the emails were subject to the common authority of Walker's employer. Walker did not enjoy any reasonable expectation of privacy vis-à-vis Penn State, and Penn State could independently consent to a search of Walker's work emails. Upon receipt of the subpoena, Penn State exercised its independent authority to consent to a search and produced Walker's work emails.[27]

Walker shows how the sale of *Carpenter*-protected business records is unregulated by the Fourth Amendment. *Carpenter*-protected business records are like Walker's emails. The user has Fourth Amendment rights in the information even as it is stored remotely on the user's server.[28] And the company that holds *Carpenter*-protected records is like Penn State. It has full access and control over the records on its server. *Walker*'s holding that the university employer has common authority over an employee's work email applies neatly to the sale of *Carpenter*-protected noncontent records generated by the business for the business's purposes that the user may not know exist and has no means to control.[29]

United States v. Ziegler[30] strikes a similar note. A private-sector employer suspected that an employee had stored evidence of crime on a workplace computer located in the employee's office at work. The employer consented to a government search of the computer for that evidence. *Ziegler* first ruled that the employee had Fourth Amendment rights in the

contents of the computer: "Because Ziegler had a reasonable expectation of privacy in his office, any search of that space and the items located therein must comply with the Fourth Amendment."[31] But the employer had access to the computer and its files: "The contents of his hard drive," the court noted, "were work-related items that contained business information and which were provided to, or created by, the employee in the context of the business relationship."[32]

Ziegler held that the employer "could consent to a search of the office and the computer that it provided to Ziegler for his work."[33] Given the employer's role, the employee "could not reasonably have expected that the computer was his personal property, free from any type of control by his employer."[34] Although *Ziegler* involves a physical computer and a physical office instead of electronic files stored on a server, as in *Walker*, the same principle applies. The computer owner retained broad access rights to the computer. The owner could therefore consent to a search of the computer that the employee used. Again, the analogy to the sale of *Carpenter*-protected records seems clear. The company that generates the records and controls their access and use has common authority that permits government access to the records.

Some readers may be wondering: What if the seller of the records did not generate them? Government access to *Carpenter*-protected records can involve many links. Provider A may generate the records of its users and then sell the records to Company B. Company B may then cull through the records and sell a subset to Company C. Company C may add in some new information and sell the resulting database to Company D, which may then sell the combined set to Company E. Does the chain of sale matter? Are the Fourth Amendment issues different if the government purchases records from Company E instead of Provider A?

I think the chain of sale does not impact third-party consent powers. Databases are valuable for the information they contain. Using the data necessarily requires access to and control over it. As a result, the company at each link in the chain will have access to and control over the data, which gives it third-party consent authority. Companies B, C, D, and E will have the same third-party consent authority as Provider A. The chain of sale might alter the Fourth Amendment analysis in other ways—for example, it might alter whether the records retain their protection under *Carpenter*—but it does not change the third-party consent analysis.

III. Could a Widespread Market in Location Records Justify a Different Result?

My argument so far is simple. But there's a slight catch that deserves a closer look. The reasoning of *Carpenter* is based on a method I have labeled "equilibrium-adjustment."[35] When technological change or social practice dramatically changes the balance of government power based on preexisting rules, the thinking runs, the Supreme Court tends to (and I think it should) adjust the old rules in an effort to restore the preexisting

equilibrium.[36] The role of equilibrium-adjustment in Fourth Amendment law generally, and in *Carpenter* specifically, raises an additional question: Will the prospect of buying databases outside the Fourth Amendment sufficiently gut *Carpenter* such that courts will or should adjust the third-party consent doctrine? Put another way, if records can be routinely bought, should courts engage in an additional equilibrium-adjustment to avoid unlimited warrantless access to *Carpenter*-protected records?

I think this is a theoretical possibility, but not, at least yet, one that courts should consider adopting. We can imagine a claim that someday there will be a need for equilibrium-adjustment to limit consent doctrine. As of the time of this writing, however, there isn't sufficient evidence that the factual predicate for such an adjustment exists. Maybe it will come someday. But today, concerns that buying databases could gut *Carpenter* are only concerns. And I don't think we have reasons to believe it will start happening soon at the scale needed to justify an additional adjustment. For the foreseeable future, at least, the willing seller rule should remain the correct approach.

Let's start with the argument that an adjustment to consent doctrine could be appropriate. Start with *Carpenter* itself. In *Carpenter*, the government collected 127 days' worth of a suspect's historical cell-site records from his cell phone provider to help show his involvement in a string of robberies. The Sixth Circuit held that this did not implicate the suspect's Fourth Amendment rights because he had voluntarily shared his location with the cell phone provider. Other circuits had reached the same result in similar cases, all of them applying the so-called third-party doctrine established by the Supreme Court in earlier cases.[37]

The Supreme Court reversed, holding that a warrant was required to compel the provider to disclose the suspect's CSLI. The Supreme Court's reasoning was based heavily on the need to maintain a balance of Fourth Amendment protection in light of technological change. Carrying a cell phone has become "indispensable to participation in modern society,"[38] the Court reasoned, and the records they automatically generated enabled "tireless and absolute surveillance"[39] of anyone. To "secure 'the privacies of life' against 'arbitrary power,'"[40] the Court could not "mechanically [apply] the third-party doctrine to this case."[41]

Carpenter made two distinct equilibrium-adjustments. First, the Court adjusted the third-party doctrine to allow users Fourth Amendment rights in their CSLI.[42] Second, the Court adjusted the usual subpoena rule to instead impose a warrant requirement to compel user records from providers.[43] The change in rules was needed to prevent the government from receiving a windfall from technological advances. "When confronting new concerns wrought by digital technology," the Court emphasized, Fourth Amendment case law "has been careful not to uncritically extend existing precedents."[44] The "seismic shifts in digital technology"[45] justified new rules to achieve "a central aim of the Framers . . . 'to place obstacles in the way of a too permeating police surveillance.'"[46]

The method of equilibrium-adjustment raises the possibility that the willing seller rule might need to be modified much like the Supreme Court modified the third-party doctrine and the subpoena rule in *Carpenter*. Here's the scenario to consider. Imagine that, for some reason, it was standard for service providers to sell CSLI to the government. Everything was for sale at a reasonable price. Investigators would always have two choices. They could compel providers to disclose records with a warrant if they had probable cause, or else they could buy the records without a warrant otherwise. The government would always have ready access to the complete location history of any person of interest. They would just need either a search warrant or dollars.

In that world, a new limit on the willing seller rule based on the equilibrium-adjustment concerns of *Carpenter* might be justified. *Carpenter* alone would no longer "place obstacles in the way of a too permeating police surveillance."[47] The market in location records would permit the "tireless and absolute surveillance"[48] that *Carpenter* tried to limit. In that circumstance, the willing seller rule might come into question for *Carpenter*-protected records. The notion of relying on third-party consent to permit a sale of *Carpenter*-protected records might become seen as "uncritically extend[ing] existing precedents" when "confronting new concerns wrought by digital technology."[49]

I don't see the evidence justifying such an adjustment now, however. That's true for three reasons: the absence of evidence that governments are relying on data purchases to get around *Carpenter* in criminal investigations to dramatically increase government power; the high bar that would need to be met for an equilibrium-adjustment; and the still-unsettled question of *Carpenter*'s scope.

The most obvious reason an additional equilibrium-adjustment would not be appropriate is the absence of public evidence that governments are commonly relying on data purchases as a substitute for a warrant under *Carpenter* in a way that has considerably altered the level of government power. *Carpenter* reflects the concern that governments can perfectly track anyone in incredible detail, reconstructing all of their movements over years. But as far as I am aware, valid concerns about the market in location records have not been matched with real cases in which buying records proved a substitute for the kind of detailed tracking at issue in *Carpenter*. Based on the public evidence, at least, the market has not proved a substitute for the kind of records access that motivated *Carpenter*.

Consider the IRS's attempted use of location information purchased from Venntel in 2017.[50] Venntel sold the IRS a subscription to access a database of user cell phone GPS location records.[51] The GPS records had been collected from cell phone apps that people had installed on their phones.[52] According to the Department of Treasury's Inspector General for Tax Administration, the subscription to Venntel's location database "was used exclusively by a single field office in the Cyber Crimes Unit, and Venntel was only utilized on a few specific occasions."[53] The access involved only two cases. And it ceased soon after, for the

simple reason that it "did not produce effective results."[54] Based on its inquiry, the Inspector General concluded that the GPS location database "did not produce useful results and was not used as a significant tool in those two investigations."[55]

This does not seem surprising, either practically or legally. Practically speaking, there is a significant gap between identifying a risk that location records could be purchased as a substitute for compelling providers and it actually happening so regularly that it has considerably expanded government power. The detailed records that could be useful in an investigation need to have been created and then stored. The owner of those records would need to be willing and able to sell them in a form that permits a buyer to link an account with a known suspect. And the government would need to know where it can purchase that information about a particular suspect and then do so.

This isn't impossible. But it isn't automatic, either, and federal privacy law makes it difficult. A brief statutory detour explains how. Companies that have *Carpenter*-protected records because they provide communications or remote storage services will generally be covered by a privacy law known as the Stored Communications Act (SCA).[56] The SCA blocks providers from disclosing noncontent records (including *Carpenter*-protected records) to the government unless a specific exception applies.[57] The exceptions closely resemble Fourth Amendment exceptions to the warrant requirement. If the government does not have a court order,[58] the customer must consent,[59] exigent circumstances must exist,[60] or some similar exception must apply.[61]

As a practical matter, the nondisclosure rule of the SCA significantly curtails the market in *Carpenter*-protected records. Although the scope of *Carpenter* is unclear—more on this in a minute—most of the records that we know to be covered by *Carpenter* will have been generated by providers covered by the SCA. Those providers cannot legally sell their records to the government. And the civil remedies of the SCA make this a serious deterrent. A provider that sells records to the government in violation of the SCA can face a class-action lawsuit filed on the behalf of its users that authorizes the award of statutory damages,[62] attorney's fees,[63] and the prospect of punitive damages for intentional violations.[64]

Some workarounds can exist, to be sure. There's always a risk of this two-step: Providers can lawfully sell their noncontent records to nongovernment data brokers,[65] and the government can then independently purchase records from the data brokers.[66] Also, other holders of *Carpenter*-protected records may be outside the SCA and can lawfully disclose.[67] Nonetheless, the SCA generally will block the government from circumventing *Carpenter* by simply buying records directly from providers. The Fourth Amendment permits it, but the SCA generally does not.

Of course, it may be that the government will purchase *Carpenter*-protected records in some cases in the future, either using existing workarounds or as a result of amendment or repeal

of the SCA nondisclosure rule. But this does not itself establish a case for altering third-party consent law based on a need for equilibrium-adjustment. Equilibrium-adjustment responds to seismic shifts, not tremors. It is justified when new technology or social practice "significantly enhances government power" or "significantly weakens police power to enforce the law."[68] The possibility that the government will buy *Carpenter*-protected records rather than obtain warrants in some cases does not justify a new consent rule to make *Carpenter* stronger unless it happens so often and so predictably that it has the practical effect of gutting the rule.

That is a high bar, as Fourth Amendment warrant requirements are always permeable. Consider the most foundational rule in Fourth Amendment law, that a warrant is needed to search a house. Despite this rule, home searches often occur without warrants. A person with common authority might consent to a search. Officers might have exigent circumstances. The fact that house searches often occur under exceptions to the warrant requirement does not render the warrant requirement for home searches meaningless. We wouldn't say that the exceptions nullify the rule and require eliminating the exceptions to make the rule meaningful. Instead, we just recognize that warrant rules always have exceptions. The same is true for *Carpenter* searches. If some protected records can be collected by third-party consent, that is not a hole in the doctrine: it is just the way the doctrine always works.

The still-uncertain scope of *Carpenter* provides a third reason why an additional equilibrium-adjustment is inappropriate for the foreseeable future. *Carpenter* remains an inkblot. This is partly because the decision is still recent. And it is partly because the good-faith exception to the exclusionary rule allowed courts to reject legal challenges to pre-*Carpenter* surveillance without reaching the merits.[69]

Whatever the reasons, cases interpreting *Carpenter* remain fairly sparse and uncertain. Much remains unknown. We don't yet know if *Carpenter* applies to all CSLI collection or just collection of many records over time. We don't know if it applies to GPS records collected from apps, such as the records accessible to the IRS in 2017 from Venntel. We don't know if it applies only to location information or to other records. Lower courts are just now trying to figure out if it extends to use of pole cameras, aerial surveillance, and other technological tools.

With the impact of *Carpenter* so uncertain, it is too early to know what records for sale might be protected under *Carpenter*. And without that knowledge, we can't yet know what hypothetical purchases of protected records are end runs around *Carpenter*'s protections. We may someday have the factual basis and legal clarity to consider an additional equilibrium-adjustment for data purchases. But it is premature to consider that now.

The sale of automated license plate reader (ALPR) records provides a helpful example. The government can purchase access to private ALPR databases.[70] This raises the prospect that

governments can buy their way around *Carpenter*. But for that to happen, we would first need to establish that equivalent access to government (as opposed to private) ALPR records would be a *Carpenter* search. As of the time of this writing, however, the case law does not establish if or when that would occur. Lower courts are divided on whether access to ALPR databases can *ever* trigger a *Carpenter* search.[71] And so far, even the courts that say a government ALPR query can in theory be a search have not identified any specific queries that are.[72]

In these circumstances, calls for equilibrium-adjustment are premature. If accessing government ALPR databases turns out to be outside the Fourth Amendment, there will be no Fourth Amendment protections to circumvent by governmental purchase of private ALPR records. There will be no need to equilibrium-adjust away from the willing seller rule. The law of what *Carpenter* protects must be established first. Whether the government is circumventing those protections in ways that require further adjustments can then follow.

Conclusion

Under current law, the Fourth Amendment law of purchasing *Carpenter*-protected records is straightforward. Because the seller will have common authority over the records, it can consent to a search. A voluntary sale amounts to voluntary consent. The need for a different rule drawing on the theory of equilibrium-adjustment may emerge someday, based on future legal and technological developments. As of 2021, however, the law is clear: government purchase of *Carpenter*-protected records from a willing seller is not an unreasonable search or seizure.

NOTES

Thanks to Jack Goldsmith and Andrew Keane Woods for comments on a prior draft.

1 138 S.Ct. 2206 (2018).

2 *See* Gilad Edelman, *Can the Government Buy Its Way Around the Fourth Amendment?*, Wired (Feb. 11, 2020, 7:00 AM), https://www.wired.com/story/can-government-buy-way-around-fourth-amendment.

3 *See infra* note 29.

4 This framework is independent of two more complex ways to approach how Fourth Amendment law applies to buying databases. One path might be to question whether particular records are protected in the first place. On its face, *Carpenter* is limited to historical cell-site location records. What other records it protects remains uncertain. *See* Orin S. Kerr, *Implementing Carpenter*, *in* The Digital Fourth Amendment (forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301257. In addition, it is unclear how the state action doctrine applies to sales of records. Depending on the facts, a seller to the government may or may not count as a state actor regulated under the Fourth Amendment. Relying on third-party consent leads to a clear answer while putting those potentially tricky issues aside. Even assuming the records are protected, and that sellers become state actors when they make exchanges with the government, buying databases still falls outside the Fourth Amendment.

5 *See generally* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561 (2009).

6 472 U.S. 463 (1985).

7 *Id*. at 469.

8 *Id*.

9 *Id*.

10 *Id*.

11 *Id*. at 470.

12 *Id*. at 471.

13 *Id*.

14 *See* Carpenter v. United States, 138 S.Ct. 2206, 2223 (2018) ("The Government's acquisition of the cell-site records here was a search under that Amendment.").

15 *See* U.S. Const. amend. IV.

16 *See generally* 4 Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment § 8.3, at 188–258 (6th ed. 2020) (discussing the law of third-party consent).

17 415 U.S. 164 (1974).

18 *Id*. at 171 n.7.

19 *See generally* Fernandez v. California, 571 U.S. 1126 (2014).

20 When the government seeks consent to search a home, the Court has carved out a narrow exception: If a co-occupant "is present at the scene and expressly refuses to consent," the government cannot rely on the consent of a different person who has common authority. Georgia v. Randolph, 547 U.S. 103, 106 (2006). This rule is based on "the ancient adage that a man's house is his castle" and traditional understandings of equality among co-tenants in a home. *Id*. at 114–15 (quoting Miller v. United States, 357 U. S. 301, 307 [1958]). This narrow exception based on traditional understandings of the home has no obvious application in the context of selling third-party business records. There is no traditional understanding that a person who buys business records is violating a norm if a person with rights in the records under *Carpenter* makes an objection known. Even the narrow *Randolph* exception requires "the objecting occupant" to be "physically present," which will not occur with a sale of records. Fernandez v. California, 571 U.S. 292, 294 (2014).

21 Carpenter v. United States, 138 S.Ct. 2206, 2211 (2018).

22 *Id*.

23 *Id*. at 2212.

24 *Id*.

25 905 F.3d 138 (3d Cir. 2018).

26 *Id*. at 149.

27 *Id*.

28 *See generally* Warshak v. United States, 631 F.3d 266 (6th Cir. 2010).

29 Although *Walker* holds that an employer had common authority over an employee's emails, I would leave for another day the precise scope of a service provider's common authority over contents. A provider might lack common authority over user contents in the same way that a landlord lacks authority to consent to an apartment

search or a hotel employee lacks authority to consent to a hotel room search. *See* Chapman v. United States, 365 U.S. 610 (1961) (landlord cannot consent to apartment search); Stoner v. California, 376 U.S. 483 (1964) (hotel clerk cannot consent to hotel room search). Terms of service might be relevant to this question, as well. *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1031 (2010) (noting but not resolving this issue). Whatever the correct answer may be for contents, the case of *Carpenter*-protected metadata is clear. This article's scope is limited to the latter.

30 474 F.3d 1184 (9th Cir. 2007).

31 *Id*. at 1190.

32 *Id*. at 1192.

33 *Id*. at 1192–93.

34 *Id*. at 1192.

35 *See generally* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 Harv. L. Rev. 476 (2011).

36 *See id*.

37 *See*, *e.g*., United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016); United States v. Davis, 785 F.3d 498, 511–13 (11th Cir. 2015); *In re* Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013)

38 Carpenter v. United States, 138 S.Ct. 2206, 2220 (2018).

39 *Id*. at 2218.

40 *Id*. at 2214.

41 *Id*. at 2219.

42 *Id*. at 2216–17.

43 *See id*. at 2221–23. For an extended discussion, *see* Orin Kerr, *Does Carpenter Revolutionize the Law of Subpoenas?*, Lawfare Blog (June 26, 2018, 6:44 PM), https://www.lawfareblog.com/does-carpenter-revolutionize-law-subpoenas.

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

45 *Id*. at 2219.

46 *Id*. at 2214 (quoting United States v. Di Re, 332 U.S. 581, 595 [1948]).

47 *See id*.

48 *See id*. at 2218.

49 *See id*. at 2222.

50 Letter from J. Russell George, Inspector General for Tax Administration, Department of Treasury, to Senators Ron Wyden and Elizabeth Warren (Feb. 18, 2021), https://s3.documentcloud.org/documents/20490079/response.pdf.

51 *Id*. at 1.

52 *Id*. at 2.

53 *Id*. at 1.

54 *Id*.

55 *Id*. at 2.

56 *See generally* Orin S. Kerr, *A User's Guide to the Stored Communications Act*, *and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208 (2004).

57 *See* 18 U.S.C. § 2702(a)(3).

58 In the case of *Carpenter*-protected records, the court order must be a warrant under the Fourth Amendment.

59 *See* 18 U.S.C. § 2702(c)(2).

60 *See* 18 U.S.C. § 2702(c)(4).

61 *See generally* 18 U.S.C. § 2702(c).

62 *See* 18 U.S.C. § 2707(c).

63 *See* 18 U.S.C. § 2707(b)(3).

64 *See* 18 U.S.C. § 2707(c).

65 *See generally* Justin Sherman, Data Brokers and Sensitive Data on U.S. Individuals (2021), https://sites.sanford.duke.edu/techpolicy/wp-content/uploads/sites/17/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf (detailing information that data brokers offer for sale on U.S. individuals).

66 The providers can sell the records to data brokers under 18 U.S.C. § 2702(c)(6), which permits disclosure to "any person other than a governmental entity," and then the government could access the records without triggering the SCA because neither § 2702 nor the compelled disclosure rules of § 2703 would apply. Exactly how much of an arms-length relationship among the various entities is needed to make this two-step process lawful has not been litigated.

67 There are also undeveloped questions about when an SCA-covered entity can anonymize data and disclose it to the government outside the SCA. The SCA's nondisclosure rule for noncontent records applies to "record[s] or other information pertaining to a subscriber to or customer of such service." *See* 18 U.S.C. § 2702(a)(3). Anonymized records or records covering large sets of customers may at some point be sufficiently distanced from any customer or subscriber so as to no longer "[pertain] to" that customer or subscriber. *Id*.

68 Kerr, *supra* note 35, at 487–88.

69 Even Carpenter himself lost on remand because of the good-faith exception. *See* United States v. Carpenter, 926 F.3d 313, 318 (6th Cir. 2019) ("The Government's acquisition of Carpenter's CSLI violated the Fourth Amendment. The district court nevertheless properly denied suppression because the FBI agents relied in good faith on the SCA when they obtained the data.").

70 *See, e.g.*, Joseph Cox, *This Company Built a Private Surveillance Network. We Tracked Someone With It*, Vice (Sept. 17, 2019), https://www.vice.com/en/article/ne879z/i-tracked-someone-with-license-plate-readers-drn.

71 *Compare* Commonwealth v. McCarthy, 142 N.E.3d 1090, 1106 (Mass. 2020) (concluding that access to data from a government ALPR database could be a search if it provided a sufficiently "detailed . . . picture of the defendant's movements"), *with* United States v. Bowers, 2021 WL 4775977 at *3 (W.D.Pa. 2021) (concluding that "[ALPR] technology is more akin to the conventional surveillance methods, such as security cameras, that the *Carpenter* Court was careful not to call into question"). *Cf.* United States v. Yang, 958 F.3d 851, 862–64 (9th Cir. 2020) (Bea, J., concurring) (speculating about whether access to a government ALPR database can be a search under *Carpenter*).

72 *See McCarthy*, 142 N.E.3d at 1106 (concluding that a query of "four [ALPR] cameras at fixed locations on the ends of two bridges" is not a search, and noting that "we cannot say precisely how detailed a picture of the defendant's movements must be revealed to invoke constitutional protections").

The views expressed in this essay are entirely those of the author and do not necessarily reflect the views of the staff, officers, or Board of Overseers of the Hoover Institution.

hoover.org

27 26 25 24 23 22 21 7 6 5 4 3 2 1

The preferred citation for this publication is Orin S. Kerr, *Buying Data and the Fourth Amendment*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2109 (November 17, 2021), available at https://www.lawfareblog.com/buying-data-and-fourth-amendment.

About the Author

ORIN S. KERR

Orin S. Kerr is a professor at the University of California–Berkeley School of Law and a nationally recognized scholar of criminal procedure and computer crime law. Kerr previously was a trial attorney in the Computer Crime and Intellectual Property Section at the Department of Justice, and a special assistant US attorney in the Eastern District of Virginia.

The Jean Perkins Foundation Working Group on National Security, Technology, and Law

The Jean Perkins Foundation Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the *Lawfare* blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith is the chair of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams /national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION