COMPUTER CRIME LAW
Fourth Edition

Summer 2018 Case Supplement

Orin S. Kerr
Frances R. and John J. Duggan Distinguished Professor
University of Southern California Gould School of Law

Author's Note:

In January 2018, West Academic Publishing published the Fourth Edition of my casebook, *Computer Crime Law*. West also published a separate 2018 Statutory Supplement at that time that contains the relevant statutes in the field. In past years, I have kept the course materials up to date with year-to-year Supplements that combine post-publication case developments and the latest statutes.

Recent events require a change in practice. A series of important changes in the law of computer crime in the last few months since publication of the Fourth Edition call for a mid-year update. This Summer 2018 Case Supplement is therefore designed to be used for the 2018-19 academic year together with the Fourth Edition of the casebook and the 2018 Statutory Supplement.

Orin Kerr
Los Angeles, CA

TABLE OF CONTENTS

CHAPTER 2

COMPUTER MISUSE CRIMES

C. UNAUTHORIZED ACCESS STATUTES

4. WHAT IS AUTHORIZATION? THE CASE OF CONTRACT-BASED RESTRICTIONS

On page 72, before Section 5, add the following new Notes 8 and 9:

8. *Does the First Amendment limit how courts must construe unauthorized access?* In Sandvig v. Sessions, __ F.Supp.3d ___, 2018 WL 1568881 (D.D.C. 2018), Judge Bates concluded that the First Amendment is relevant to how courts construe the CFAA in the context of public websites. In *Sandvig*, a group of researchers who regularly visit public websites in violation of their Terms of Service for academic research purposes filed a civil suit against the Attorney General of the United States challenging the constitutionality of the CFAA on a range of grounds including the First Amendment. The government responded that the First Amendment does not apply because the CFAA only regulates the computer owner's private property.

Judge Bates began by explaining why the First Amendment might limit how the CFAA applies to visiting a website available to the public even though the computer is privately owned:

> Stroll out onto the National Mall [in Washington, D.C.] on any day with decent weather and you will discover a phalanx of food trucks lining the streets. Those food trucks are privately owned businesses. Customers interact with them for the private purpose of buying a meal. If they were a brick-and-mortar store on private property, they would encounter no First Amendment barrier to removing a patron who created a ruckus. Yet if a customer standing on a public sidewalk tastes her food and then yells at those in line behind her that they should avail themselves of the myriad other culinary options nearby, the truck could not call the police to arrest her for her comments. She is in a public forum, and her speech remains protected even when she interacts with a private business located within that forum.
>
> It makes good sense to treat the Internet in this manner. Each medium of expression must be assessed for First Amendment purposes by standards suited to it, for each may present its own problems. Regulation of the Internet presents serious line-drawing problems that the public/private distinction in physical space does not. [Supreme Court decisions limiting the First Amendment on private property] concerned property privately owned and used nondiscriminatorily for private purposes only. It is difficult to argue that most websites readily meet this description. . . . . Simply put: the public Internet is too heavily suffused with First Amendment activity, and what might otherwise be deemed private spaces are too blurred with expressive spaces, to sustain a direct parallel to the physical world.

According to Judge Bates, the First Amendment does not apply to computer access that circumvents a code-based restriction but it may require a narrow construction of unauthorized access when no code-based restriction is involved:

> Rifling through a business's confidential files is no less a trespass merely because those files are located in the cloud. A hacker cannot legally break into a Gmail account and copy the account-holder's emails, just as a busybody cannot legally reach into someone else's mailbox and open her mail. The First Amendment does not give someone the right to breach a paywall on a news website any more than it gives someone the right to steal a newspaper.
>
> What separates these examples . . is that the owners of the information at issue have taken real steps to limit who can access it. But simply placing contractual conditions on accounts that anyone can create, as social media and many other sites do, does not remove a website from the First Amendment protections of the public Internet. Rather, only code-based restrictions, which carve out a virtual private space within the website or service that requires proper authentication to gain access, remove those protected portions of a site from the public forum. Stealing another's credentials, or breaching a site's security to evade a code-based restriction, therefore remains unprotected by the First Amendment.

If the First Amendment limits how courts interpret unauthorized access, what limits should it impose?

9. *Creating fictitious user accounts under the CFAA*. Imagine a website allows anyone to register for an account on the condition, expressed in the terms of service, that they must provide their real names and identities on registration. Anyone with an account can enter a username and password to see nonpublic information available to those with accounts. Imagine a user creates an account using a fictitious identity, and he uses that account to access nonpublic information on the website. Does the act of accessing the information using the account count as bypassing a code-based restriction (because it was used to access hidden information), or is it merely violating a contractual restriction (because it violated the terms of service)? And does that classification determine whether they violate the CFAA?

In Sandvig v. Sessions, __ F.Supp.3d ___, 2018 WL 1568881 (D.D.C. 2018), a group of researchers regularly visited public websites for academic purposes in ways that violated the websites' terms of service. In some cases, they created fictitious accounts before using the accounts to gather information. Applying the narrow interpretation of exceeding authorized access from *Nosal*, Judge Bates concluded that merely visiting public websites in violation of terms of service, as well as using "bots" to access the sites in violation of terms of service, was authorized. "Employing a bot to crawl a website or apply for jobs," Judge Bates explained, "may run afoul of a website's ToS, but it does not constitute an access violation when the human who creates the bot is otherwise allowed to read and interact with that site." On the other hand, creating a fictitious user account could exceed authorized access:

> Unlike plaintiffs' other conduct, which occurs on portions of websites that any visitor can view, creating false accounts allows [a computer user] to access information on those sites that is both limited to those who meet the owners' chosen authentication requirements and targeted to the particular preferences of the user. Creating false accounts and obtaining information through those accounts would

> therefore [be a prohibited act of exceeding authorized access.]

In a footnote, Judge Bates added:

> Professor Kerr argues that "a website that appears to require a username and password to access the contents of the site, but that actually grants access for any username and password combination," should not be seen as creating an access restriction, because it "would appear to a user to regulate by code, but would actually work more like a system of regulation by contract." Kerr, *Cybercrime's Scope*, supra, at 1646. The distinction between code-based and contract-based barriers matters for First Amendment analysis, but it does not quite line up with the Court's reading of the CFAA. Social media sites like Facebook, for instance, grant access for any username and password combination, but they still allow those with accounts to access data that those who merely visit the site without signing up cannot. Hence, conditions placed on account creation can still be access restrictions.

F. 18 U.S.C. § 1030(A)(5) AND COMPUTER DAMAGE STATUTES

1. 18 U.S.C. §1030(A)(5) MISDEMEANOR LIABILITY

At the bottom of page 109, replace *United States v. Carlson* with the following new decision:

18 U.S.C. § 1030(a)(5)(A) is different from other provisions of § 1030 because it prohibits unauthorized damage instead of unauthorized access. This raises obvious questions: When is a person authorized to damage a computer? How clear must authorization be, and how can it be provided? The following recent case sheds light on the answers.

UNITED STATES V. THOMAS

United States Court of Appeals for the Fifth Circuit, 2017.
877 F.3d 591.

GREGG COSTA, CIRCUIT JUDGE.

Michael Thomas worked as the Information Technology Operations Manager for ClickMotive, LP, a software and webpage hosting company. Upset that a coworker had been fired, Thomas embarked on a weekend campaign of electronic sabotage. He deleted over 600 files, disabled backup operations, eliminated employees from a group email a client used to contact the company, diverted executives' emails to his personal account, and set a "time bomb" that would result in employees being unable to remotely access the company's network after Thomas submitted his resignation. Once ClickMotive discovered what Thomas did, it incurred over $130,000 in costs to fix these problems.

A jury found Thomas guilty of knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causing damage without authorization, to a protected computer. 18 U.S.C. § 1030(a)(5)(A). Thomas challenges the "without authorization" requirement of this provision of the Computer Fraud and Abuse Act. He contends that because his IT job gave him full access to the system and required him to "damage" the system—for example, at times his duties included deleting certain files—his conduct did not lack authorization. But we conclude that Thomas's conduct falls squarely within the ordinary meaning of the statute and affirm his conviction.

I.

Thomas's duties at ClickMotive included network administration; maintaining production websites; installing, maintaining, upgrading, and troubleshooting network servers; ensuring system security and data integrity; and performing backups. He was granted full access to the network operating system and had the authority to access any data and change any setting on the system. Thomas was expected to perform his duties using his "best efforts and judgment to produce maximum benefit" to ClickMotive.

Thomas was not happy when his friend in the IT department was fired. It was not just a matter of loyalty to his former colleague; a smaller IT staff meant more work for Thomas. So

Thomas, to use his word, "tinkered" with the company's system. The tinkering, which started on a Friday evening and continued through Monday morning, included the following:

- He deleted 625 files of backup history and deleted automated commands set to perform future backups.
- He issued a command to destroy the virtual machine[1] that performed ClickMotive's backups for one of its servers and then Thomas failed to activate its redundant pair, ensuring that the backups would not occur.
- He tampered with ClickMotive's pager notification system by entering false contact information for various company employees, ensuring that they would not receive any automatically-generated alerts indicating system problems.
- He triggered automatic forwarding of executives' emails to an external personal email account he created during the weekend.
- He deleted pages from ClickMotive's internal "wiki," an online system of internal policies and procedures that employees routinely used for troubleshooting computer problems.
- He manually changed the setting for an authentication service that would eventually lead to the inability of employees to work remotely through VPN. Changing the setting of the VPN authentication service set a time bomb that would cause the VPN to become inoperative when someone rebooted the system, a common and foreseeable maintenance function.
- And he removed employees from e-mail distribution groups created for the benefit of customers, leading to customers' requests for support going unnoticed.

Thomas was able to engage in most of this conduct from home, but he did set the VPN time bomb on Sunday evening from ClickMotive's office, which he entered using another employee's credentials. It was during this visit to the office that Thomas left his resignation letter that the company would see the next day. When the dust settled, the company incurred over $130,000 in out-of-pocket expenses and employees' time to undo the harm Thomas caused. In a subsequent interview with the FBI, Thomas stated that he engaged in this conduct because he was "frustrated" with the company and wanted to make the job harder for the person who would replace him.

A grand jury eventually charged Thomas with the section 1030(a)(5)(A) offense. But two days before the grand jury met, Thomas fled to Brazil. Nearly three years later, Thomas was arrested when he surrendered to FBI agents at Dallas/Fort Worth International Airport.

At trial, company employees and outside IT experts testified that none of the problems ClickMotive experienced as a result of Thomas's actions would be attributable to a normal system malfunction. They further stated that Thomas's actions were not consistent with normal troubleshooting and maintenance or consistent with mistakes made by a novice. ClickMotive employees asserted that it was strange for the wiki pages to be missing and that someone in Thomas's position would know that changing the setting of the VPN authentication service would cause it to become inoperative when someone rebooted the system.

ClickMotive's employee handbook was not offered at trial and there was no specific company policy that governed the deletions of backups, virtual machines, or wiki modifications. Employees explained, however, that there were policies prohibiting interfering with ClickMotive's

normal course of business and the destruction of its assets, such as a virtual machine or company data. Thomas's own Employment Agreement specified he was bound by policies that were reasonably necessary to protect ClickMotive's legitimate interests in its clients, customers, accounts, and work product.

The jury instructions included the statutory definition of "damage," which is "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). The district court denied Thomas's proposed instruction for "without authorization," which was "without permission or authority." It did not define the phrase.

After the jury returned a guilty verdict, the district court sentenced Thomas to time served (which was the four months since he had been detained after returning to the country), plus three years of supervised release, and ordered restitution of $131,391.21.

II.

A.

Because Thomas's argument that he was authorized to damage a computer seems nonsensical at first glance, it is helpful at the outset to explain the steps he takes to get there. He first points out that his job duties included "routinely deleting data, removing programs, and taking systems offline for diagnosis and maintenance." Thomas says this conduct damaged the computer within the meaning of the Computer Fraud and Abuse Act because damage is defined to just mean "any impairment to the integrity or availability of data, a program, a system, or information," 18 U.S.C. § 1030(e)(8); there is no requirement of harm. And the damage he caused by engaging in these routine tasks was not "without authorization" because it was part of his job. So far, so good.

Next comes the critical leap: Thomas argues that because he was authorized to damage the computer when engaging in these routine tasks, *any* damage he caused while an employee was not "without authorization." Thus he cannot be prosecuted under section 1030(a)(5)(A). This argument is far reaching. If Thomas is correct, then the damage statute would not reach any employee who intentionally damaged a computer system as long as any part of that employee's job included deleting files or taking systems offline.

Thomas's support for reading the statute to cover only individuals who had no rights, limited or otherwise to impair a system comes from cases addressing the separate "access" provisions of section 1030. *See, e.g.*, *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009) ("A person who uses a computer 'without authorization' has no rights, limited or otherwise, to access the computer in question."). But there are important differences between the "access" and "damage" crimes that make it inappropriate to import access caselaw into the damage statute.

Section 1030(a)(5)(A) is the only independent "damage" provision, meaning it does not also require a lack of authorization to access the computer. *Contrast* 18 U.S.C. § 1030(a)(5)(B), (C) (both applying to damage that results from unauthorized access of a computer). It prohibits intentionally causing damage without authorization. As discussed, the statute defines damage. And as numerous courts have recognized in discussing both the damage and access provisions, the ordinary meaning of "without authorization" is "without permission." Indeed, Thomas asked that the jury be told that "without authorization" means "without permission or authority"; he did not

seek an instruction that "without authorization" is limited to those who have no rights to ever impair a system.

As the caselaw and Thomas's proposed instruction recognize, the plain meaning of the damage provision is that it makes it a crime to intentionally impair a computer system without permission. And notably, it applies to particular acts causing damage that lacked authorization. *See* 18 U.S.C. § 1030(e)(8) (defining damage to include a single impairment of the system). Nothing in the statutory text says it does not apply to intentional acts of damage that lacked permission if the employee was allowed to engage at other times in other acts that impaired the system.

"Without authorization" modifies damage rather than access. Section 1030(a)(5)(A) makes no distinction between all-or-nothing authorization and degrees of authorization. Its text therefore covers situations when the individual never had permission to damage the system (an outsider) or when someone who might have permission for some damaging acts causes other damage that is not authorized (an insider). Tellingly, other subsections of the same damage statute are limited to those who inflict damage while "intentionally access[ing] a protected computer without authorization." 18 U.S.C. § 1030(a)(5)(B), (C). Because section 1030(a)(5)(A) is the one subsection of the damage statute that also applies to insiders, it would make no sense to import a limitation from the access statutes that is aimed at excluding insider liability.

Nor is there a significant threat that liability under the damage statute would extend to largely innocuous conduct because the requirement of "intentionally causing damage" narrows the statute's reach.

We conclude that Section 1030(a)(5)(A) prohibits intentionally damaging a computer system when there was no permission to engage in that particular act of damage. To the extent more is needed to flesh out the scope of "permission" when a defendant has some general authority to impair a network, there is helpful guidance in one of our cases addressing an access statute, which if anything should define authorization more narrowly for the reasons we have discussed. *United States v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007). *Phillips* says to look at the expected norms of intended use.

B.

There is overwhelming evidence to support the jury's view that Thomas did not have permission to engage in the weekend damage campaign.

The nature of Thomas's conduct is highly incriminating. No reasonable employee could think he had permission to stop the system from providing backups, or to delete files outside the normal protocols, or to falsify contact information in a notification system, or to set a process in motion that would prevent users from remotely accessing the network. Thomas emphasizes the unlimited access he had to the system that gave him the ability to inflict this damage. But it is not conceivable that any employee, regardless of their level of computer access, would be authorized to cause these problems. The incidents for which Thomas was held liable were nothing like the periodic acts he performed as part of his duties. Those tasks may have impaired the system on a limited basis in order to benefit the computer network in the long run. Routine deletions of old files provide that benefit by increasing storage space. Taking systems offline allows for necessary maintenance.

In contrast, the various types of damage Thomas caused during the last few days before he resigned resulted in over $130,000 in remediation costs. Regardless of whether the definition of "damage" under the statute requires a showing of harm, impairments that harm the system are much less likely to be authorized than those that benefit the system. It would rarely if ever make sense for an employer to authorize an employee to harm its computer system.

The harmful acts themselves would be enough to support the verdict, but Thomas's words and conduct in response to the criminal investigation provide additional support. When questioned by federal agents, he acknowledged the distinction we have just made. He did not say that he caused the damage in order to maintain or improve the system; instead, his motive was to make things more difficult for the person hired to replace him. And his flight to Brazil is not what is expected of someone who had permission to engage in the conduct being investigated.

The circumstances surrounding the damaging acts provide even more support for the finding of guilt. Thomas committed the various acts one after the other in a concentrated time span beginning Friday evening and continuing through the weekend. Thomas did most of this from home, but the one time he had to go the office he did so using another employee's credentials. One of his acts—falsification of contact information in the alert system—prevented Thomas's conduct from being detected during the weekend as employees would not receive notifications about the damage to the system. He submitted his resignation immediately after completing the damage spree and timed the most damaging act—the one that would prevent remote access—so that it would not occur until he was gone. Why this sequence of events if Thomas had permission to cause the damage? All of this provided ample support to conclude that Thomas lacked permission to inflict the damage he caused.

The judgment of the district court is affirmed.

CHAPTER 3

TRADITIONAL CRIMES

A. ECONOMIC CRIMES

1. PROPERTY CRIMES

On page 159, at the end of Note 5, add the following material as an addendum to Note 5:

On appeal to the New York Court of Appeals, New York's highest state court, the court affirmed the conviction. *See* People v. Aleynikov, ___ N.E.3d ____, 2018 WL 2048707 (N.Y. 2018). The Court of Appeals agreed with the Appellate Division that Aleynikov made a "tangible reproduction" by copying the source code:

> Ideas begin in the mind. By its very nature, an idea, be it a symphony or computer source code, begins as intangible property. However, the medium upon which an idea is stored is generally physical, whether it is represented on a computer hard drive, vinyl record, or compact disc. The changes made to a hard drive or disc when information is copied onto it are physical in nature. The representation occupies space. Consequently, a statute that criminalizes the making of a tangible reproduction or representation of secret scientific material by electronically copying or recording applies to the acts of a defendant who uploads proprietary source code to a computer server.
>
> A rational jury could have found that the "reproduction or representation" that defendant made of Goldman's source code, when he uploaded it to the German server, was tangible in the sense of "material" or "having physical form." The jury heard testimony that the representation of source code has physical form. Kumar, the computer engineer, testified that while source code, as abstract intellectual property, does not have physical form, the representation of it is material. He explained that when computer files are stored on a hard drive or CD, they are physically present on that hard drive or disc, and further stated that data is visible in aggregate when stored on such a medium. The jury also heard testimony that source code that is stored on a computer takes up physical space in a computer hard drive. Given that a reproduction of computer code takes up space on a drive, it is clear that it is physical in nature. In short, the changes that are made to the hard drive or disc, when code or other information is stored, are physical.

B. CRIMES AGAINST PERSONS
1. THREATS AND HARASSMENT
C) REVENGE PORN LAWS

On the top of page 248, add the following new Note 3:

3. *Another "revenge porn" law struck down on First Amendment grounds*. In Ex parte Jones, ___ S.W.3d___, 2018 WL 2228888 (Tx. Ct. App. 2018), the Texas Court of Appeals invalidated a recently-enacted state revenge pornography law. The law, Tex. Penal Code § 21.16(b), reads as follows:

> A person commits an offense if:
> (1) without the effective consent of the depicted person, the person intentionally discloses visual material depicting another person with the person's intimate parts exposed or engaged in sexual conduct;
> (2) the visual material was obtained by the person or created under circumstances in which the depicted person had a reasonable expectation that the visual material would remain private;
> (3) the disclosure of the visual material causes harm to the depicted person; and
> (4) the disclosure of the visual material reveals the identity of the depicted person in any manner.

In defending the statute against a First Amendment facial challenge, the state conceded that the law was a regulation of speech that was not content-neutral. The court accepted the concession and agreed with it: "Section 21.16(b)(1) penalizes only a subset of disclosed images, those which depict another person with the person's intimate parts exposed or engaged in sexual conduct. Therefore, we conclude that Section 21.16(b)(1) discriminates on the basis of content." So construed, the court held, the Texas law was subject to strict scrutiny that it could not pass: "Because Section 21.16(b) does not use the least restrictive means of achieving what we have assumed to be the compelling government interest of preventing the intolerable invasion of a substantial privacy interest, it is an invalid content-based restriction in violation of the First Amendment."

According to the court, the biggest problem with the statute was the disjunctive test in Section 21.16(b)(2). That language required that "the visual material was obtained by the person *or* created under circumstances in which the depicted person had a reasonable expectation that the visual material would remain private" (emphasis added). The difficulty with this language, the court explained, is that a person could be liable under the statute even if they did not know that the depicted person had a reasonable expectation that the visual material would remain private. The court explained the flaw in the statute with the following hypothetical:

> Adam and Barbara are in a committed relationship. One evening, in their home, during a moment of passion, Adam asks Barbara if he can take a nude photograph of her. Barbara consents, but before Adam takes the picture, she tells him that he must not show the photograph to anyone else. Adam promises that he will never

> show the picture to another living soul, and takes a photograph of Barbara in front of a plain, white background with her breasts exposed.
>
> A few months pass, and Adam and Barbara break up after Adam discovers that Barbara has had an affair. A few weeks later, Adam rediscovers the topless photo he took of Barbara. Feeling angry and betrayed, Adam emails the photo without comment to several of his friends, including Charlie. Charlie never had met Barbara and, therefore, does not recognize her. But he likes the photograph and forwards the email without comment to some of his friends, one of whom, unbeknownst to Charlie, is Barbara's coworker, Donna. Donna recognizes Barbara and shows the picture to Barbara's supervisor, who terminates Barbara's employment.
>
> Meanwhile, Adam also emails the picture to Ed. This time, however, Adam writes in the body of the email, "She thought I never would show anyone." Ed reads the email and forwards it with the attachment to several friends.
>
> In this scenario, Adam and Ed can be charged under Section 21.16(b), but so can Charlie and Donna. Charlie has a First Amendment right to share a photograph. Charlie had no reason to know that the photograph was created under circumstances under which Barbara had a reasonable expectation that the photograph would remain private. Charlie was not aware of Barbara's conditions posed to Adam immediately prior to the photograph's creation, nor did he receive the photograph with any commentary from Adam that would make him aware of this privacy expectation on Barbara's part.
>
> In fact, there is nothing to suggest that Charlie could not reasonably have believed that Adam found this picture on a public website or had been given permission by the depicted person to share the image with others. Further still, Charlie did not intend to harm the depicted person. Lastly, Charlie did not and could not identify the depicted person because he did not know Barbara. Yet, under the disjunctive language used in Section 21.16(b)(2), Charlie nonetheless is culpable despite his having no knowledge of the circumstances surrounding the photograph's creation or the depicted person's privacy expectation arising thereunder.

Although the court struck down the statute on the ground that it did not use the least restrictive means of protecting privacy, the court also found that the statute was fatally overbroad:

> Section 21.16 is extremely broad, applying to any person who discloses visual material depicting another person's intimate parts or a person engaged in sexual conduct, but where the disclosing person has no knowledge or reason to know the circumstances surrounding the material's creation, under which the depicted person's reasonable expectation of privacy arose. Furthermore, its application is not attenuated by the fact that the disclosing person had no intent to harm the depicted person or may have been unaware of the depicted person's identity.

If the court's First Amendment analysis is correct, do you think the constitutional defect would be cured if the statute added a statutory requirement of intent to harm?

C. VICE CRIMES

On page 283, before the beginning of Part D., add the following new subsection:

3. PROSTITUTION

In April 2018, Congress enacted a new federal law designed to limit the use of websites that further prostitution. Here is the new law, now codified at 18 U.S.C. § 2421A:

> *§ 2421A. Promotion or facilitation of prostitution and reckless disregard of sex trafficking*
>
> **(a) In general.**--Whoever, using a facility or means of interstate or foreign commerce or in or affecting interstate or foreign commerce, owns, manages, or operates an interactive computer service (as such term is defined in defined in section 230(f) the Communications Act of 1934 (47 U.S.C. 230(f))), or conspires or attempts to do so, with the intent to promote or facilitate the prostitution of another person shall be fined under this title, imprisoned for not more than 10 years, or both.
> **(b) Aggravated violation.**--Whoever, using a facility or means of interstate or foreign commerce or in or affecting interstate or foreign commerce, owns, manages, or operates an interactive computer service (as such term is defined in defined in section 230(f) the Communications Act of 1934 (47 U.S.C. 230(f))), or conspires or attempts to do so, with the intent to promote or facilitate the prostitution of another person and--
>
> **(1)** promotes or facilitates the prostitution of 5 or more persons; or
> **(2)** acts in reckless disregard of the fact that such conduct contributed to sex trafficking, in violation of 1591(a),
>
> shall be fined under this title, imprisoned for not more than 25 years, or both.
> **(c) Civil recovery.**--Any person injured by reason of a violation of section 2421A(b) may recover damages and reasonable attorneys' fees in an action before any appropriate United States district court.
> **(d) Mandatory restitution.**--Notwithstanding sections 3663 or 3663A and in addition to any other civil or criminal penalties authorized by law, the court shall order restitution for any violation of subsection (b)(2). The scope and nature of such restitution shall be consistent with section 2327(b).
> **(e) Affirmative defense.**--It shall be an affirmative defense to a charge of violating subsection (a), or subsection (b)(1) where the defendant proves, by a preponderance of the evidence, that the promotion or facilitation of prostitution is legal in the jurisdiction where the promotion or facilitation was targeted.

Pub.L. 115-164, § 3(a), Apr. 11, 2018, 132 Stat. 1253.

Notes and Questions

1. 18 U.S.C. § 2421A(a) was passed as part of the Allow States And Victims To Fight Online Sex Trafficking Act, Pub. L. 115-164, known colloquially as "FOSTA." The passage of FOSTA reflects a concern that authorities lacked the tools to combat prostitution and sex trafficking online. In particular, websites such as Backpage.com hosted thousands of prostitution advertisements. Much of the new statute is addressed to limiting the immunity of such websites against civil and state liability under Section 230 of the Communications Decency Act. But part of the law also includes this new federal criminal provision. Do you think the new federal law was necessary? Should running a website that promotes prostitution be left to state law, or is it appropriate for Congress to punish such conduct at the federal level?

2. *Interactive computer service.* 47 U.S.C. § 230(f)(2) defines "interactive computer service" as

> any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

Under this definition, a website is the most common type of interactive computer service. *See* Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157, 1163 n.6 (9th Cir. 2003). As a result, the prohibition in 18 U.S.C. § 2421A(a) has the effect of making it a federal crime to own, manage, or operate a website with the intent of furthering illegal prostitution.

3. *The affirmative defense.* Like most vice crimes, prostitution is typically a matter of state law rather than federal law. To that end, the new statute provides an affirmative defense to a charge of violating subsection (a), or subsection (b)(1), "where the defendant proves, by a preponderance of the evidence, that the promotion or facilitation of prostitution is legal in the jurisdiction where the promotion or facilitation was targeted."

Compare the affirmative defense in § 2421A(e) to the somewhat analogous treatment of state law in the context of the federal prohibition on running an interstate sports betting operation in violation of the Wire Act, 18 U.S.C. § 1084. Recall from the materials on Internet gambling that the Wire Act provides the following exception:

> Nothing in this section shall be construed to prevent the transmission in interstate or foreign commerce of information for use in news reporting of sporting events or contests, or for the transmission of information assisting in the placing of bets or wagers on a sporting event or contest from a State or foreign country where betting on that sporting event or contest is legal into a State or foreign country in which such betting is legal.

18 U.S.C. § 1084(b). The text of this provision, as construed in the *Cohen* case on page 255 of your casebook, suggests that the government has the burden of showing that gambling is illegal according to at least one of the laws of the state or country where the bet was placed or received. In contrast, § 2421A(e) places the burden on the defendant to show by a preponderance of the evidence that the promotion or facilitation of prostitution is legal. Which is the better approach? Does it matter in practice, given that the issue is the state of the law rather than a fact?

CHAPTER 4

SENTENCING

C. SENTENCING IN COMPUTER MISUSE CASES

On page 383 at the bottom, add the following new Note 11:

11. *Enhancements for "substantial disruption of a critical infrastructure."* Section 2B1.1(b)(18)(A)(iii) provides a six-level enhancement for a violation of § 1030 that causes a "substantial disruption of a critical infrastructure." (Note that page 372 of your casebook lists this language as being in Section 2B1.1(b)(17). Recent changes to 2B1.1 not relevant to our discussion have since moved this text to 2B1.1(b)(18). The language remains the same.) The harsh extra penalty when a § 1030 violation substantially disrupts a critical infrastructure raises obvious interpretive questions: When does a computer count as a critical infrastructure, and what is the standard for when a CFAA violation substantially disrupts it?

The Fifth Circuit answered these questions in United States v. Brown, 884 F.3d 281 (5th Cir. 2018). The defendant, a system specialist at Citibank's Global Control Center, reacted to a negative review of his job performance by sending commands that intentionally disrupted network traffic on Citibank's network. The defendant's act of sabotage, which started at about 6pm, resulted in a loss of connectivity to some but not all of Citibank's North American data centers, campuses, call centers, and sixty-nine ATMs. By about 10 p.m., Citibank was able to restore ninety percent of the lost connectivity. By 4:30 a.m. the next morning, the network was back up and running normally. At sentencing, the trial court applied the enhancement for substantial disruption of a critical infrastructure.

On appeal, the Fifth Circuit ruled that this enhancement was improperly applied to the facts of Brown's case. On one hand, it was clear from the Guidelines definition that Citibank's computers involved critical infrastructure:

> The commentary to the 2015 Sentencing Guidelines defines "critical infrastructure" as "systems and assets vital to national defense, national security, economic security, public health or safety, or any combination of these matters." U.S. Sentencing Guidelines Manual § 2B1.1(b)(18) cmt. n.14 (U.S. Sentencing Comm'n 2015). The enumerated examples include public and private "financing and banking systems."

Id. at 285. Despite this, the enhancement was improperly applied because Brown's conduct did not cause a "substantial disruption" of that critical infrastructure:

> Brown's conduct did not constitute a substantial disruption of a critical infrastructure. There is no indication that Brown's conduct affecting a portion of Citibank's operations for a short period of time could have had a serious impact on national economic security. As a result of Brown's actions, Citibank suffered

> relatively minor financial losses and was temporarily unable to optimally serve its customers. Neither of these harms threatened to disrupt the nation's economy, and, in light of Citibank's demonstrated ability to quickly resolve the disruption and mitigate in the interim, there is no other evidence that Brown's conduct had the potential to do so. Accordingly, we hold that the district court erred by applying an enhancement that we conclude is reserved for conduct that disrupts a critical infrastructure in a way that could have a serious impact on national economic security.

Id. at 287.

CHAPTER 5

THE FOURTH AMENDMENT

B. DEFINING SEARCHES AND SEIZURES

1. SEARCHES

C) SEARCHES IN THE NETWORK CONTEXT

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

CARPENTER V. UNITED STATES

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

CHIEF JUSTICE ROBERTS delivered the opinion of the Court.

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

I

A

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

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

Wireless carriers collect and store CSLI for their own business purposes, including finding weak spots in their network and applying "roaming" charges when another carrier routes data through their cell sites. In addition, wireless carriers often sell aggregated location records to data

brokers, without individual identifying information of the sort at issue here. While carriers have long retained CSLI for the start and end of incoming calls, in recent years phone companies have also collected location information from the transmission of text messages and routine data connections. Accordingly, modern cell phones generate increasingly vast amounts of increasingly precise CSLI.

B

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

Based on that information, the prosecutors applied for court orders under the Stored Communications Act to obtain cell phone records for petitioner Timothy Carpenter and several other suspects. That statute, as amended in 1994, permits the Government to compel the disclosure of certain telecommunications records when it "offers specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Federal Magistrate Judges issued two orders directing Carpenter's wireless carriers—MetroPCS and Sprint—to disclose cell/site sector information for Carpenter's telephone at call origination and at call termination for incoming and outgoing calls during the four-month period when the string of robberies occurred. The first order sought 152 days of cell-site records from MetroPCS, which produced records spanning 127 days. The second order requested seven days of CSLI from Sprint, which produced two days of records covering the period when Carpenter's phone was "roaming" in northeastern Ohio. Altogether the Government obtained 12,898 location points cataloging Carpenter's movements—an average of 101 data points per day.

Carpenter was charged with six counts of robbery and an additional six counts of carrying a firearm during a federal crime of violence. At trial, seven of Carpenter's confederates pegged him as the leader of the operation. In addition, FBI agent Christopher Hess offered expert testimony about the cell-site data. Hess explained that each time a cell phone taps into the wireless network, the carrier logs a time-stamped record of the cell site and particular sector that were used. With this information, Hess produced maps that placed Carpenter's phone near four of the charged robberies. In the Government's view, the location records clinched the case: They confirmed that Carpenter was "right where the robbery was at the exact time of the robbery." App. 131 (closing argument). Carpenter was convicted on all but one of the firearm counts and sentenced to more than 100 years in prison.

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

II

A

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

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

B

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

The first set of cases addresses a person's expectation of privacy in his physical location and movements. In *United States v. Knotts,* 460 U.S. 276 (1983), we considered the Government's use of a "beeper" to aid in tracking a vehicle through traffic. Police officers in that case planted a beeper in a container of chloroform before it was purchased by one of Knotts's co-conspirators. The officers (with intermittent aerial assistance) then followed the automobile carrying the container from Minneapolis to Knotts's cabin in Wisconsin, relying on the beeper's signal to help keep the vehicle in view. The Court concluded that the augmented visual surveillance did not constitute a search because a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. Since the movements of the vehicle and its final destination had been voluntarily conveyed to anyone who wanted to look, Knotts could not assert a privacy interest in the information obtained.

This Court in *Knotts,* however, was careful to distinguish between the rudimentary tracking facilitated by the beeper and more sweeping modes of surveillance. The Court emphasized the limited use which the government made of the signals from this particular beeper during a discrete automotive journey. Significantly, the Court reserved the question whether different constitutional principles may be applicable if twenty-four hour surveillance of any citizen of this country were possible.

Three decades later, the Court considered more sophisticated surveillance of the sort envisioned in *Knotts* and found that different principles did indeed apply. In *United States v. Jones,* 565 U.S. 400 (2012), FBI agents installed a GPS tracking device on Jones's vehicle and remotely monitored the vehicle's movements for 28 days. The Court decided the case based on the

Government's physical trespass of the vehicle. At the same time, five Justices agreed that related privacy concerns would be raised by, for example, surreptitiously activating a stolen vehicle detection system in Jones's car to track Jones himself, or conducting GPS tracking of his cell phone. *Id.,* at 426, 428 (Alito, J., concurring in judgment); *id.,* at 415 (Sotomayor, J., concurring). Since GPS monitoring of a vehicle tracks every movement a person makes in that vehicle, the concurring Justices concluded that longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy—regardless whether those movements were disclosed to the public at large. *Id.,* at 430, (opinion of Alito, J.); *id.,* at 415 (opinion of Sotomayor, J.).

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

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

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

III

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

At the same time, the fact that the individual continuously reveals his location to his wireless carrier implicates the third-party principle of *Smith* and *Miller*. But while the third-party

doctrine applies to telephone numbers and bank records, it is not clear whether its logic extends to the qualitatively different category of cell-site records. After all, when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements.

We decline to extend *Smith* and *Miller* to cover these novel circumstances. Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection. Whether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. The location information obtained from Carpenter's wireless carriers was the product of a search.[3]

A

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

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

In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones*. Unlike the bugged container in *Knotts* or the car in *Jones,* a cell phone—almost a feature of human anatomy —tracks nearly exactly the movements of its owner. While individuals regularly leave their vehicles, they compulsively carry cell phones

[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. 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. 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.

with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales. Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user.

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

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

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

Accordingly, when the Government accessed CSLI from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements.

B

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

The Government's position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years. Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible. There is a world of difference between the limited types of

personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today. The Government thus is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information.

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

The Court has in fact already shown special solicitude for location information in the third-party context. In *Knotts,* the Court relied on *Smith* to hold that an individual has no reasonable expectation of privacy in public movements that he "voluntarily conveyed to anyone who wanted to look. But when confronted with more pervasive tracking, five Justices [in *Jones*] agreed that longer term GPS monitoring of even a vehicle traveling on public streets constitutes a search. [T]his case is not about "using a phone" or a person's movement at a particular time. It is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years. Such a chronicle implicates privacy concerns far beyond those considered in *Smith* and *Miller*.

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

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

* * *

Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or "tower dumps" (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith*

and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security.

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

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

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

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

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

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

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

control, or use the records, and for that reason have no reasonable expectation that they cannot be disclosed pursuant to lawful compulsory process.

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

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

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

JUSTICE GORSUCH, dissenting.

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

I cannot fault the Sixth Circuit for holding that *Smith* and *Miller* extinguish any *Katz*-based Fourth Amendment interest in third party cell-site data. That is the plain effect of their categorical holdings. Nor can I fault the Court today for its implicit but unmistakable conclusion that the rationale of *Smith* and *Miller* is wrong; indeed, I agree with that. The Sixth Circuit was powerless to say so, but this Court can and should. At the same time, I do not agree with the Court's decision today to keep *Smith* and *Miller* on life support and supplement them with a new and multilayered inquiry that seems to be only *Katz*-squared. Returning there, I worry, promises more trouble than help. Instead, I would look to a more traditional Fourth Amendment approach. Even if *Katz* may

still supply one way to prove a Fourth Amendment interest, it has never been the only way. Neglecting more traditional approaches may mean failing to vindicate the full protections of the Fourth Amendment.

Notes and Questions

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

How should courts apply this distinction to Internet surveillance? For example, consider the surveillance of IP addresses in *United States v. Forrester* on pages 425-48 of your casebook. *Forrester* relied on a direct analogy to *Smith v. Maryland*. The Ninth Circuit reasoned that IP addresses are just the Internet equivalent of numbers dialed. But that was in 2007. Should *Carpenter* lead to a different result today? Is the government's power to observe the address of every website a person visits over time a new power that has caused a "seismic shift" in government power? Or is IP address monitoring merely a "traditional" surveillance technique because IP addresses are just the Internet version of telephone numbers dialed? Does it make a difference if IP addresses are not stored and are only available in real time? Does it matter how much information is revealed by an IP address?

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

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

3. *Short-term vs. long-term surveillance*. Footnote 3 of *Carpenter* states that the Court "need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be." The distinction between long-term and short-term surveillance was the basis of Justice Alito's concurring opinion in *Jones,* on which the reasoning of *Carpenter* is based. In *Jones*, the government installed a physical GPS device on a car the suspect was driving and tracked the car's

location for 28 days. Justice Alito reasoned that using the GPS device only briefly was not a search because that was the kind of government surveillance people have long expected. Longer term surveillance became a search, Justice Alito reasoned, because it was the kind of surveillance that people wouldn't expect the government to be able to conduct. Here's the key language from Justice Alito's *Jones* concurrence:

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

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

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

C. EXCEPTIONS TO THE WARRRANT REQUIREMENT

4. BORDER SEARCHES

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

8. *Federal circuits divide on applying the border search exception to computers*. In May 2018, decisions from the Fourth Circuit and Eleventh Circuit reached different conclusions on how to apply the border exception to computers. The new decisions create a clear disagreement among lower courts that often prompts review from the United States Supreme Court.

First, in United States v. Kolsuz, 890 F.3d 133 (4th Cir. 2018), the Fourth Circuit held that forensic searches of computers at the border require some kind of suspicion. The Fourth Circuit's decision, authored by Judge Pamela Harris, did not resolve exactly how much suspicion was required — whether reasonable suspicion was sufficient as *Cotterman* had held, or if probable cause was needed, or even if the legal process of a warrant was necessary. But echoing the Ninth Circuit's decision in *Cotterman*, the Fourth Circuit in *Kolsuz* rejected the notion that forensic searches of computers could be allowed without any suspicion at all. Much of the reasoning in *Kolsuz* tracked the Ninth Circuit's reasoning in *Cotterman*, which the Fourth Circuit argued was bolstered by the Supreme Court's subsequent decision in *Riley v. California*, 134 S.Ct. 2473 (2014):

> And then came *Riley*, in which the Supreme Court confirmed every particular of [the reasoning in *Cotterman*]. *Riley* holds that the search incident to arrest exception, which allows for automatic searches of personal effects in the possession of an arrestee, does not apply to manual searches of cell phones. The key to *Riley*'s reasoning is its express refusal to treat such phones as just another form of container, like the wallets, bags, address books, and diaries covered by the search incident exception. Instead, *Riley* insists, cell phones are fundamentally different in both a quantitative and a qualitative sense from other objects traditionally subject to government searches.
>
> And that is so, *Riley* explains, for precisely the reasons already identified by cases treating border searches of digital devices as nonroutine: the immense storage capacity of cell phones, putting a vastly larger array of information at risk of exposure; the special sensitivity of the kinds of information that may be stored on a phone, such as browsing history and historical location data; and, finally, the element of pervasiveness that characterizes cell phones, making them an "insistent part of daily life.
>
> After *Riley*, we think it is clear that a forensic search of a digital phone must be treated as a nonroutine border search, requiring some form of individualized suspicion.

Id. at 146. Notably, *Kolsuz* left open the possibility that there is also an individualized suspicion requirement for a manual search of a computer at the border. *See id.* at n.5 ("Because Kolsuz does not challenge the initial manual search of his phone at Dulles, we have no occasion here to consider whether *Riley* calls into question the permissibility of suspicionless manual searches of digital devices at the border.")

Two weeks after the Fourth Circuit handed down *Kolsuz*, the Eleventh Circuit adopted a very different approach in United States v. Touset, 890 F.3d 1227 (11th Cir. 2018). In a decision by Judge William Pryor, the Eleventh Circuit held that no suspicion is required for a border search of a computer whether it is a manual or forensic search:

> We see no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property. Just as the United States is entitled to search a fuel tank for drugs, it is entitled to search a flash drive for child pornography. And it does not make sense to say that electronic devices should receive special treatment because so many people now own them or because they can store vast quantities of records or effects. The same could be said for a recreational vehicle filled with personal effects or a tractor-trailer loaded with boxes of documents. Border agents bear the same responsibility for preventing the importation of contraband in a traveler's possession regardless of advances in technology. Indeed, inspection of a traveler's property at the border is an old practice and is intimately associated with excluding illegal articles from the country.
>
> In contrast with searches of property, we have required reasonable suspicion at the border only for highly intrusive searches of a person's body. Even though the Supreme Court has declined to decide what level of suspicion, if any, is required for such nonroutine border searches of a person, [our Eleventh Circuit caselaw has] required reasonable suspicion for a strip search or an x-ray examination. We have defined the intrusiveness of a search of a person's body that requires reasonable suspicion in terms of the indignity that will be suffered by the person being searched in contrast with whether one search will reveal more than another. And we have isolated three factors which contribute to the personal indignity endured by the person searched: (1) physical contact between the searcher and the person searched; (2) exposure of intimate body parts; and (3) use of force.
>
> These factors are irrelevant to searches of electronic devices. A forensic search of an electronic device is not like a strip search or an x-ray; it does not require border agents to touch a traveler's body, to expose intimate body parts, or to use any physical force against him. Although it may intrude on the privacy of the owner, a forensic search of an electronic device is a search of property. And our precedents do not require suspicion for intrusive searches of any property at the border.

Id. at 1234. Judge Pryor's opinion in *Touset* recognizes the Eleventh Circuit disagreement with the Ninth Circuit in *Cotterman* and the Fourth Circuit's decision in *Kolsuz*.

> Although the Supreme Court stressed in *Riley* that the search of a cell phone risks a significant intrusion on privacy, *Riley* does not apply to searches at the border. And our precedent considers only the personal indignity of a search, not its extensiveness. Again, we fail to see how the personal nature of data stored on electronic devices could trigger this kind of indignity when our precedent establishes that a suspicionless search of a home at the border does not. Property and persons are different.

> We are also unpersuaded that a traveler's privacy interest should be given greater weight than the paramount interest of the sovereign in protecting its territorial integrity. The Ninth and Fourth Circuits stressed the former interest and asserted that travelers have no practical options to protect their privacy when traveling abroad. For example, the Ninth Circuit explained that it is "impractical, if not impossible, for individuals to make meaningful decisions regarding what digital content to expose to the scrutiny that accompanies international travel" and that "removing files unnecessary to an impending trip" is "a time-consuming task that may not even effectively erase the files." *Cotterman*, 709 F.3d at 965. The Fourth Circuit added that "it is neither realistic nor reasonable to expect the average traveler to leave his digital devices at home when traveling." *Kolsuz*, 890 F.3d at 145.
>
> But a traveler's expectation of privacy is less at the border, and the Fourth Amendment does not guarantee the right to travel without great inconvenience, even within our borders. Anyone who has recently taken a domestic flight likely experienced inconvenient screening procedures that require passengers to unpack electronic devices, separate and limit liquids, gels, and creams, remove their shoes, and walk through a full-body scanner. Travelers crossing a border are on notice that a search may be made, and they are free to leave any property they do not want searched—unlike their bodies—at home.
>
> In contrast with the diminished privacy interests of travelers, the government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border. Nothing in *Riley* undermines this interest. In *Riley*, the Supreme Court explained that the rationales that support the search-incident-to-arrest exception—namely the concerns of harm to officers and destruction of evidence—did not have much force with respect to digital content on cell phones, because digital data does not pose comparable risks. But digital child pornography [involved in *Touset*] poses the same exact risk of unlawful entry at the border as its physical counterpart. If anything, the advent of sophisticated technological means for concealing contraband only heightens the need of the government to search property at the border unencumbered by judicial second-guessing.
>
> Indeed, if we were to require reasonable suspicion for searches of electronic devices, we would create special protection for the property most often used to store and disseminate child pornography. With the advent of the internet, child pornography offenses overwhelmingly involve the use of electronic devices for the receipt, storage, and distribution of unlawful images. And law enforcement officers routinely investigate child-pornography offenses by forensically searching an individual's electronic devices. We see no reason why we would permit traditional, invasive searches of all other kinds of property, but create a special rule that will benefit offenders who now conceal contraband in a new kind of property.

Id. at 1234-35.

Where does that leave us? After *Cotterman*, *Kolsuz*, and *Touset*, the law of computer border searches in the Ninth, Fourth, and Eleventh Circuits can be summarized by the following chart:

	Ninth Circuit (Cotterman)	*Fourth Circuit (Kolsuz)*	*Eleventh Circuit (Touset)*
Manual Search at the Border	No suspicion required	Undecided	No suspicion required
Forensic Search at the Border	Reasonable suspicion required	Some individualized suspicion required, although undecided how much	No suspicion required

If the Supreme Court agrees to decide how the Fourth Amendment applies to border searches, how should the Supreme Court rule? Should there be a different answer for manual searches and forensic searches? Or should there be one answer for all computer searches – and if so, what should it be?

9. *More on the distinction between manual and forensic searches.* The Fourth Circuit offered additional clarification on the distinction between "manual" and "forensic" searches in United States v. Kolsuz, 890 F.3d 133 (4th Cir. 2018). Recall from Note 2 on page 514 of your casebook that *Kolsuz* involved the use of a Cellebrite Universal Forensic Extraction Device Physical Analyzer to extract 896 printed pages of data from a cell phone. The Fourth Circuit agreed with the district court that this was a forensic search. The Fourth Circuit further explained the distinction by reference to a new computer border search policy enacted by the Department of Homeland Security:

> Shortly after argument in this case, the Department of Homeland Security adopted a policy that treats forensic searches of digital devices as nonroutine border searches, insofar as such searches now may be conducted only with reasonable suspicion of activity that violates the customs laws or in cases raising national security concerns. U.S. Customs and Border Prot., CBP Directive No. 3340-049A, Border Search of Electronic Devices 5 (2018).
>
> The new policy does not use the "routine" and "nonroutine" terminology of Supreme Court case law, distinguishing instead between "basic" and "advanced" searches. But the import is the same. "Basic" searches (like those we term "manual") are examinations of an electronic device that do not entail the use of external equipment or software and may be conducted without suspicion. "Advanced" searches (like "forensic" searches) involve the connection of external equipment to a device – such as the Cellebrite Physical Analyzer used on Kolsuz's phone – in order to review, copy, or analyze its contents, and are subject to the restrictions noted above.

Id. at 146, 146 n.6. At least in the Fourth Circuit, then, the distinction between manual and forensic searches appears to hinge on whether the search involves the use of external equipment (or perhaps the use of external software).

CHAPTER 6

STATUTORY PRIVACY PROTECTIONS

D. THE STORED COMMUNICATIONS ACT

3. VOLUNTARY DISCLOSURES UNDER 2702

On page 716, add the following citation at the end of Note 10:

See also Facebook v. Superior Court, 4 Cal.5th 1245, 1282-85 (Cal. 2018) (agreeing with the reasoning of *Negro*).

On page 718, add the following new Note 15:

15. *The consent exception and public postings.* Imagine a private party issues a subpoena to Facebook directing Facebook to disclose status updates that the user had posted on his Facebook wall. Imagine some of the status updates were configured to be visible to the general public, while other status updates were configured so that they could be viewed only by the person's Facebook friends. Must Facebook comply with the subpoena, or is compliance blocked by the Stored Communications Act?

In Facebook v. Superior Court, 4 Cal.5th 1245 (Cal. 2018), the Supreme Court of California held that the answer depends on the privacy settings of the status update. If the privacy settings are set to public, the court reasoned, then the posting of the contents in a way available to the public amounts to consent to disclosure that is permitted by the implied consent provision of 18 U.S.C. 2702(b)(3). *See id*. at 1274-7. On the other hand, if the posting is restricted, then there is no implied consent. That is true, the court held, even if "a communication was configured by the user to be accessible to a large group of friends or followers." *Id*. at 1281.

Do you agree that a user's privacy settings can create implied consent to disclose communications? If so, what is the relevant timeframe for consent? Users can change the privacy settings for particular communications at any time. Imagine a user posts a public status update in 2016. Two years later, in 2018, the user is embroiled in litigation and restricts the post to friends only. Does the 2018 restriction amount to a withdrawal of consent?

CHAPTER 7

JURISDICTION

C. INTERNATIONAL COMPUTER CRIMES

2. STATUTORY PRIVACY LAWS

On page 791, replace Notes 1-3 with the following new Note on the Cloud Act:

1. *Congress resolves the Microsoft issue by enacting the CLOUD Act*. Congress passed a new law in March 2018 to resolve the question in the *Microsoft* case. The new law, the Clarifying Lawful Overseas Use of Data Act ("CLOUD") Act, was enacted as part of the Consolidated Appropriations Act, 2018, Pub. L. 115–141. The CLOUD Act requires a provider to disclose contents or records "regardless of whether such communication, record, or other information is located within or outside the United States." 18 U.S.C. § 2713. In that sense, the new statute reflects the government's goal in the *Microsoft* litigation. Providers now cannot refuse to comply with domestic legal process based on the foreign location of stored data.

At the same time, the CLOUD Act gives providers a limited statutory basis on which to challenge domestic legal process that involves a conflict with foreign law. The provider has 14 days to file a motion to quash or modify the legal process on the grounds of a perceived conflict of law. The circumstances in which this challenge can succeed are very narrow, however. Under 18 U.S.C. § 2703(h)(2)(A), a provider can file a challenge to domestic legal process only when the following five conditions are all met:

> (1) the domestic legal process is seeking the contents of communications;
>
> (2) the provider reasonably believes that the customer or subscriber is not a United States person;
>
> (3) the provider reasonably believes that the customer or subscriber does not reside in the United States; and
>
> (4) the disclosure implicates the law of a foreign government that has been designated a "qualifying foreign government"; and
>
> (5) the provider reasonably believes that the required disclosure would create a material risk that the provider would violate the law of the qualifying foreign government.

The concept of a "qualifying foreign government" is explained in the new Note below. As the new Note explains, a "qualifying foreign government" essentially refers to a foreign governments with U.S.-like privacy laws that has been pre-approved as having sufficient privacy protection to permit mutual legal compliance.

After hearing a response from the government, the court can modify or quash (that is, annul) legal process under this provision only if the court makes three findings:

> (i) the required disclosure would cause the provider to violate the laws of a qualifying foreign government;
>
> (ii) based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and
>
> (iii) the customer or subscriber is not a United States person and does not reside in the United States.

18 U.S.C. § 2703(h)(2)(B).

The "interests of justice" factors are detailed in 18 U.S.C. § 2703(h)(3). Courts should consider, "as appropriate," the following eight factors:

> (A) the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure;
>
> (B) the interests of the qualifying foreign government in preventing any prohibited disclosure;
>
> (C) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider;
>
> (D) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States, or if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the nature and extent of the subscriber or customer's connection to the foreign authority's country;
>
> (E) the nature and extent of the provider's ties to and presence in the United States;
>
> (F) the importance to the investigation of the information required to be disclosed;
>
> (G) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and
>
> (H) if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the investigative interests of the foreign authority making the request for assistance.

Note that the basis for challenging domestic legal process under the CLOUD Act is exceedingly narrow. The provider must take the initiative and file the challenge. The disclosure must be unlawful under the law of a government that has been designated a "qualifying foreign government." The interests of justice must favor quashing or modifying the legal process. And the account holder must be a non-U.S. person who does not reside in the United States. If any of these requirements has not been met, the domestic legal process is binding on the provider despite the foreign law implications of the process.

How often is that likely to happen?

C. INTERNATIONAL COMPUTER CRIMES
2. MUTUAL LEGAL ASSISTANCE AND INTERNATIONAL TREATIES

On page 817, replace Note 6 with the following new Notes 6 and 6.1:

6. *Congress creates a new regime for cross-border data requests.* In March 2018, Congress created a new legal framework for cross-border data requests with pre-approved foreign governments as part of the Clarifying Lawful Overseas Use of Data Act ("CLOUD") Act. Under the new statute, the United States government can determine that a foreign government is a "qualifying foreign government." *See* 18 U.S.C. § 2523 (establishing the process). When a U.S. provider receives foreign legal process from a qualifying foreign government, new exceptions to the U.S. surveillance laws permit the provider to comply with the foreign legal process without violating U.S. law.

Importantly, the CLOUD Act does not require the provider to comply with foreign legal process. The legal burden to comply with the foreign legal process comes, if at all, from the law of the foreign government. Instead, the CLOUD Act removes the federal legal prohibition on compliance with the foreign legal process so long as the foreign government has been declared a "qualifying foreign government" under the process provided by 18 U.S.C. § 2523.

To achieve this result, the CLOUD Act adds new exceptions to each of three major federal statutory surveillance laws for conduct in response to foreign legal process. *See, e.g.,* 18 U.S.C. § 2702(b)(9) (new exception to the Stored Communications Act permits disclosure of contents "to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523"); 18 U.S.C. § 2702(b)(9) (new exception to the Stored Communications Act permits disclosure of non-content records "to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523"); 18 U.S.C. § 2511(j) (new exception to the Wiretap Act permitting "a provider of electronic communication service to the public or remote computing service to intercept or disclose the contents of a wire or electronic communication in response to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523."); 18 U.S.C. § 3121(a) (new exception to the Pen Register statute permits installation of a pen register and trap and trace device pursuant to "an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.").

The effect of the CLOUD Act is to create an "insider's club" among countries in terms of legal process. When a foreign government is admitted into the club by being designated a "qualifying foreign government," evidence collection using foreign legal process becomes relatively easy. Domestic providers can follow foreign court orders – the foreign equivalent of their Wiretap orders, 2703(a) warrants, and pen/trap orders – just like they follow domestic legal process. And under the reciprocity requirements that are part of being a "qualifying foreign government" – as explained in Note 6.1 below – domestic legal process can be followed by foreign providers just like they now comply with foreign legal process.

6.1 *Becoming a "qualifying foreign government" under 18 U.S.C. § 2523*. The CLOUD Act's regime for cross-border data requests hinges on designation of a foreign government as a "qualifying foreign government." The procedure for this designation is detailed in 18 U.S.C. § 2523. The procedure is complex. The full statute appears at the end of this supplement, but the basics can be readily understood here. First, the foreign government must enter into an executive agreement with the United States concerning mutual legal assistance that satisfies a long list of statutory requirements. When the executive agreement is made, the Attorney General, with the concurrence of the Secretary of State, then submits a written certification of such determination to Congress, that a foreign government is properly qualifying. Congress then has an opportunity to reject the agreement. If Congress does not act after 180 days, the executive agreement goes into effect and the foreign government is a "qualifying foreign government" for five years.

The terms of the executive agreement are explained in § 2523(b). First, "the domestic law of the foreign government, including the implementation of that law, [must] afford[] robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement." § 2523(b)(1). Factors to be consider to determine if the foreign government's laws and practices are adequate in that regard include whether the government demonstrates respect for the rule of law and principles of nondiscrimination; whether it adheres to applicable international human rights obligations and commitments or demonstrates respect for international universal human rights; and whether it has sufficient mechanisms to provide accountability and appropriate transparency regarding the collection and use of electronic data . *See id.* at § 2523(b)(1)(B).

The executive agreements must also be mutual. Just as the United States will permit U.S.-based providers to comply with foreign legal process, so must the foreign governments permit their providers to comply with U.S. legal process. *See* § 2523(b)(4)(I) ("[T]he foreign government shall afford reciprocal rights of data access, to include, where applicable, removing restrictions on communications service providers, including providers subject to United States jurisdiction, and thereby allow them to respond to valid legal process sought by a governmental entity (as defined in section 2711) if foreign law would otherwise prohibit communications-service providers from disclosing the data.").

After the Attorney General certifies that a valid executive agreement exists, the Attorney General must submit the certification to Congress. Congress then has 180 days in which to consider the executive agreement. If Congress has not acted in 180 days, the agreement goes into effect. *See* § 2523(d). On the other hand, if Congress enters a joint resolution in the 180-day period disapproving of the executive agreement, then the executive agreement does not go into effect. *See* § 2523(d)(4)(B). Executive agreements are valid for five years and can be renewed for additional five-year periods. If revisions are made to the executive agreements as part of their proposed renewal, the Attorney General must resubmit the revised executive agreement to Congress to give Congress a 90-day window in which to consider the agreement. *See* § 2523(h).

RELEVANT TEXT OF THE CLOUD ACT

The CLOUD Act makes many changes to the electronic surveillance laws that are interspersed throughout the statutory privacy laws. There are three major new provisions: 18 U.S.C. § 2523 (on the procedure for establishing qualifying legal governments), 18 U.S.C. § 2713 (the requirement of complying with legal process regardless of storage location), and 18 U.S.C. § 2703(h) (on the procedure for challenging domestic legal process based on possible conflict with foreign law).

The text of the three major provisions is below. It begins with § 2523, and the text of § 2713 and § 2703(h) begin on page 44.

18 U.S.C. § 2523.
Executive agreements on access to data by foreign governments

(a) Definitions.--In this section--

> **(1)** the term "lawfully admitted for permanent residence" has the meaning given the term in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a)); and
>
> **(2)** the term "United States person" means a citizen or national of the United States, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the United States.

(b) Executive agreement requirements.--For purposes of this chapter, chapter 121, and chapter 206, an executive agreement governing access by a foreign government to data subject to this chapter, chapter 121, or chapter 206 shall be considered to satisfy the requirements of this section if the Attorney General, with the concurrence of the Secretary of State, determines, and submits a written certification of such determination to Congress, including a written certification and explanation of each consideration in paragraphs (1), (2), (3), and (4), that--

> **(1)** the domestic law of the foreign government, including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement, if--
>
> > **(A)** such a determination under this section takes into account, as appropriate, credible information and expert input; and
> >
> > **(B)** the factors to be met in making such a determination include whether the foreign government--
> >
> > **(i)** has adequate substantive and procedural laws on cybercrime and electronic evidence, as demonstrated by being a party to the Convention on Cybercrime, done at Budapest November 23, 2001, and entered into force January 7, 2004, or through domestic laws that are consistent with definitions and the requirements set forth in chapters I and II of that Convention;
> >
> > **(ii)** demonstrates respect for the rule of law and principles of nondiscrimination;
> >
> > **(iii)** adheres to applicable international human rights obligations and commitments or demonstrates respect for international universal human rights, including--

(I) protection from arbitrary and unlawful interference with privacy;

(II) fair trial rights;

(III) freedom of expression, association, and peaceful assembly;

(IV) prohibitions on arbitrary arrest and detention; and

(V) prohibitions against torture and cruel, inhuman, or degrading treatment or punishment;

(iv) has clear legal mandates and procedures governing those entities of the foreign government that are authorized to seek data under the executive agreement, including procedures through which those authorities collect, retain, use, and share data, and effective oversight of these activities;

(v) has sufficient mechanisms to provide accountability and appropriate transparency regarding the collection and use of electronic data by the foreign government; and

(vi) demonstrates a commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the Internet;

(2) the foreign government has adopted appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons subject to the agreement;

(3) the terms of the agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data; and

(4) the agreement requires that, with respect to any order that is subject to the agreement--

(A) the foreign government may not intentionally target a United States person or a person located in the United States, and shall adopt targeting procedures designed to meet this requirement;

(B) the foreign government may not target a non-United States person located outside the United States if the purpose is to obtain information concerning a United States person or a person located in the United States;

(C) the foreign government may not issue an order at the request of or to obtain information to provide to the United States Government or a third-party government, nor shall the foreign government be required to share any information produced with the United States Government or a third-party government;

(D) an order issued by the foreign government--

(i) shall be for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism;

(ii) shall identify a specific person, account, address, or personal device, or any other specific identifier as the object of the order;

(iii) shall be in compliance with the domestic law of that country, and any obligation for a provider of an electronic communications service or a remote computing service to produce data shall derive solely from that law;

(iv) shall be based on requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation;

(v) shall be subject to review or oversight by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the order; and

(vi) in the case of an order for the interception of wire or electronic communications, and any extensions thereof, shall require that the interception order--

(I) be for a fixed, limited duration; and

(II) may not last longer than is reasonably necessary to accomplish the approved purposes of the order; and

(III) be issued only if the same information could not reasonably be obtained by another less intrusive method;

(E) an order issued by the foreign government may not be used to infringe freedom of speech;

(F) the foreign government shall promptly review material collected pursuant to the agreement and store any unreviewed communications on a secure system accessible only to those persons trained in applicable procedures;

(G) the foreign government shall, using procedures that, to the maximum extent possible, meet the definition of minimization procedures in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801), segregate, seal, or delete, and not disseminate material found not to be information that is, or is necessary to understand or assess the importance of information that is, relevant to the prevention, detection, investigation, or prosecution of serious crime, including terrorism, or necessary to protect against a threat of death or serious bodily harm to any person;

(H) the foreign government may not disseminate the content of a communication of a United States person to United States authorities unless the communication may be disseminated pursuant to subparagraph (G) and relates to significant harm, or the threat thereof, to the United States or United States persons, including crimes involving national security such as terrorism, significant violent crime, child exploitation, transnational organized crime, or significant financial fraud;

(I) the foreign government shall afford reciprocal rights of data access, to include, where applicable, removing restrictions on communications service providers, including providers subject to United States jurisdiction, and thereby allow them to respond to valid legal process sought by a governmental entity (as defined in section 2711) if foreign law would otherwise prohibit communications-service providers from disclosing the data;

(J) the foreign government shall agree to periodic review of compliance by the foreign government with the terms of the agreement to be conducted by the United States Government; and

(K) the United States Government shall reserve the right to render the agreement inapplicable as to any order for which the United States Government concludes the agreement may not properly be invoked.

(c) Limitation on judicial review.--A determination or certification made by the Attorney General under subsection (b) shall not be subject to judicial or administrative review.

(d) Effective date of certification.--

(1) Notice.--Not later than 7 days after the date on which the Attorney General certifies an executive agreement under subsection (b), the Attorney General shall provide notice of the determination under subsection (b) and a copy of the executive agreement to Congress, including--

(A) the Committee on the Judiciary and the Committee on Foreign Relations of the Senate; and

(B) the Committee on the Judiciary and the Committee on Foreign Affairs of the House of Representatives.

(2) Entry into force.--An executive agreement that is determined and certified by the Attorney General to satisfy the requirements of this section shall enter into force not earlier than the date that is 180 days after the date on which notice is provided under paragraph (1), unless Congress enacts a joint resolution of disapproval in accordance with paragraph (4).

(3) Requests for information.--Upon request by the Chairman or Ranking Member of a congressional committee described in paragraph (1), the head of an agency shall promptly furnish a summary of factors considered in determining that the foreign government satisfies the requirements of this section.

(4) Congressional review.--

(A) Joint resolution defined.--In this paragraph, the term "joint resolution" means only a joint resolution--

(i) introduced during the 180-day period described in paragraph (2);

(ii) which does not have a preamble;

(iii) the title of which is as follows: "Joint resolution disapproving the executive agreement signed by the United States and ___.", the blank space being appropriately filled in; and

(iv) the matter after the resolving clause of which is as follows: "That Congress disapproves the executive agreement governing access by ____ to certain electronic data as submitted by the Attorney General on ____", the blank spaces being appropriately filled in.

(B) Joint resolution enacted.--Notwithstanding any other provision of this section, if not later than 180 days after the date on which notice is provided to Congress under paragraph (1), there is enacted into law a joint resolution disapproving of an executive agreement under this section, the executive agreement shall not enter into force.

(C) Introduction.--During the 180-day period described in subparagraph (B), a joint resolution of disapproval may be introduced--

(i) in the House of Representatives, by the majority leader or the minority leader; and

(ii) in the Senate, by the majority leader (or the majority leader's designee) or the minority leader (or the minority leader's designee).

(5) Floor consideration in House of Representatives.--If a committee of the House of Representatives to which a joint resolution of disapproval has been referred has not reported the joint resolution within 120 days after the date of referral, that committee shall be discharged from further consideration of the joint resolution.

(6) Consideration in the Senate.--

(A) Committee referral.--A joint resolution of disapproval introduced in the Senate shall be referred jointly--

(i) to the Committee on the Judiciary; and

(ii) to the Committee on Foreign Relations.

(B) Reporting and discharge.--If a committee to which a joint resolution of disapproval was referred has not reported the joint resolution within 120 days after the date of referral of the joint resolution, that committee shall be discharged from further consideration of the joint resolution and the joint resolution shall be placed on the appropriate calendar.

(C) Proceeding to consideration.--It is in order at any time after both the Committee on the Judiciary and the Committee on Foreign Relations report a joint resolution of disapproval to the Senate or have been discharged from consideration of such a joint resolution (even though a previous motion to the same effect has been disagreed to) to move to proceed to the consideration of the joint resolution, and all points of order against the joint resolution (and against consideration of the joint resolution) are waived. The motion is not debatable or subject to a motion to postpone. A motion to reconsider the vote by which the motion is agreed to or disagreed to shall not be in order.

(D) Consideration in the Senate.--In the Senate, consideration of the joint resolution, and on all debatable motions and appeals in connection therewith, shall be limited to not more than 10 hours, which shall be divided equally between those favoring and those opposing the joint resolution. A motion further to limit debate is in order and not debatable. An amendment to, or a motion to postpone, or a motion to proceed to the consideration of other business, or a motion to recommit the joint resolution is not in order.

(E) Consideration of veto messages.--Debate in the Senate of any veto message with respect to a joint resolution of disapproval, including all debatable motions and appeals in connection with the joint resolution, shall be limited to 10 hours, to be equally divided between, and controlled by, the majority leader and the minority leader or their designees.

(7) Rules relating to Senate and House of Representatives.--

(A) Treatment of Senate Joint Resolution in House.--In the House of Representatives, the following procedures shall apply to a joint resolution of disapproval received from the Senate (unless the House has already passed a joint resolution relating to the same proposed action):

(i) The joint resolution shall be referred to the appropriate committees.

(ii) If a committee to which a joint resolution has been referred has not reported the joint resolution within 7 days after the date of referral, that committee shall be discharged from further consideration of the joint resolution.

(iii) Beginning on the third legislative day after each committee to which a joint resolution has been referred reports the joint resolution to the House or has been discharged from further consideration thereof, it shall be in order to move to proceed to consider the joint resolution in the House. All points of order against the motion are waived. Such a motion shall not be in order after the House has disposed of a motion to proceed on the joint resolution. The previous question shall be considered as ordered on the motion to its adoption without intervening motion. The motion shall not be debatable. A motion to reconsider the vote by which the motion is disposed of shall not be in order.

(iv) The joint resolution shall be considered as read. All points of order against the joint resolution and against its consideration are waived. The previous question shall be considered as ordered on the joint resolution to final passage without intervening motion except 2 hours of debate equally divided and controlled by the sponsor of the joint resolution (or a designee) and an opponent. A motion to reconsider the vote on passage of the joint resolution shall not be in order.

(B) Treatment of House Joint Resolution in Senate.--

(i) If, before the passage by the Senate of a joint resolution of disapproval, the Senate receives an identical joint resolution from the House of Representatives, the following procedures shall apply:

(I) That joint resolution shall not be referred to a committee.

(II) With respect to that joint resolution--

(aa) the procedure in the Senate shall be the same as if no joint resolution had been received from the House of Representatives; but

(bb) the vote on passage shall be on the joint resolution from the House of Representatives.

(ii) If, following passage of a joint resolution of disapproval in the Senate, the Senate receives an identical joint resolution from the House of Representatives, that joint resolution shall be placed on the appropriate Senate calendar.

(iii) If a joint resolution of disapproval is received from the House, and no companion joint resolution has been introduced in the Senate, the Senate procedures under this subsection shall apply to the House joint resolution.

(C) Application to revenue measures.--The provisions of this paragraph shall not apply in the House of Representatives to a joint resolution of disapproval that is a revenue measure.

(8) Rules of House of Representatives and Senate.--This subsection is enacted by Congress--

(A) as an exercise of the rulemaking power of the Senate and the House of Representatives, respectively, and as such is deemed a part of the rules of each House,

respectively, and supersedes other rules only to the extent that it is inconsistent with such rules; and

(B) with full recognition of the constitutional right of either House to change the rules (so far as relating to the procedure of that House) at any time, in the same manner, and to the same extent as in the case of any other rule of that House.

(e) Renewal of determination.--

(1) In general.--The Attorney General, with the concurrence of the Secretary of State, shall review and may renew a determination under subsection (b) every 5 years.
(2) Report.--Upon renewing a determination under subsection (b), the Attorney General shall file a report with the Committee on the Judiciary and the Committee on Foreign Relations of the Senate and the Committee on the Judiciary and the Committee on Foreign Affairs of the House of Representatives describing--
(A) the reasons for the renewal;
(B) any substantive changes to the agreement or to the relevant laws or procedures of the foreign government since the original determination or, in the case of a second or subsequent renewal, since the last renewal; and
(C) how the agreement has been implemented and what problems or controversies, if any, have arisen as a result of the agreement or its implementation.

(3) Nonrenewal.--If a determination is not renewed under paragraph (1), the agreement shall no longer be considered to satisfy the requirements of this section.

(f) Revisions to agreement.--A revision to an agreement under this section shall be treated as a new agreement for purposes of this section and shall be subject to the certification requirement under subsection (b), and to the procedures under subsection (d), except that for purposes of a revision to an agreement--

(1) the applicable time period under paragraphs (2), (4)(A)(i), (4)(B), and (4)(C) of subsection (d) shall be 90 days after the date notice is provided under subsection (d)(1); and
(2) the applicable time period under paragraphs (5) and (6)(B) of subsection (d) shall be 60 days after the date notice is provided under subsection (d)(1).

(g) Publication.--Any determination or certification under subsection (b) regarding an executive agreement under this section, including any termination or renewal of such an agreement, shall be published in the Federal Register as soon as is reasonably practicable.

(h) Minimization procedures.--A United States authority that receives the content of a communication described in subsection (b)(4)(H) from a foreign government in accordance with an executive agreement under this section shall use procedures that, to the maximum extent possible, meet the definition of minimization procedures in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801) to appropriately protect nonpublicly available information concerning United States persons.

18 U.S.C. § 2713
Required preservation and disclosure of communications and records

A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.

18 U.S.C. § 2703(h)
Comity analysis and disclosure of information regarding legal process seeking contents of wire or electronic communication.

(1) Definitions.--In this subsection--

(A) the term "qualifying foreign government" means a foreign government--

(i) with which the United States has an executive agreement that has entered into force under section 2523; and

(ii) the laws of which provide to electronic communication service providers and remote computing service providers substantive and procedural opportunities similar to those provided under paragraphs (2) and (5); and

(B) the term "United States person" has the meaning given the term in section 2523.

(2) Motions to quash or modify.—

(A) A provider of electronic communication service to the public or remote computing service, including a foreign electronic communication service or remote computing service, that is being required to disclose pursuant to legal process issued under this section the contents of a wire or electronic communication of a subscriber or customer, may file a motion to modify or quash the legal process where the provider reasonably believes--

(i) that the customer or subscriber is not a United States person and does not reside in the United States; and

(ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government.

Such a motion shall be filed not later than 14 days after the date on which the provider was served with the legal process, absent agreement with the government or permission from the court to extend the deadline based on an application made within the 14 days. The right to move to quash is without prejudice to any other grounds to move to quash or defenses thereto, but it shall be the sole basis for moving to quash on the grounds of a conflict of law related to a qualifying foreign government.

(B) Upon receipt of a motion filed pursuant to subparagraph (A), the court shall afford the governmental entity that applied for or issued the legal process under this section the opportunity to respond. The court may modify or quash the legal process, as appropriate, only if the court finds that--

(i) the required disclosure would cause the provider to violate the laws of a qualifying foreign government;

(ii) based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and

(iii) the customer or subscriber is not a United States person and does not reside in the United States.

(3) Comity analysis.--For purposes of making a determination under paragraph (2)(B)(ii), the court shall take into account, as appropriate--

(A) the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure;

(B) the interests of the qualifying foreign government in preventing any prohibited disclosure;

(C) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider;

(D) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States, or if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the nature and extent of the subscriber or customer's connection to the foreign authority's country;

(E) the nature and extent of the provider's ties to and presence in the United States;

(F) the importance to the investigation of the information required to be disclosed;

(G) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and

(H) if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the investigative interests of the foreign authority making the request for assistance.

(4) Disclosure obligations during pendency of challenge.--A service provider shall preserve, but not be obligated to produce, information sought during the pendency of a motion brought under this subsection, unless the court finds that immediate production is necessary to prevent an adverse result identified in section 2705(a)(2).

(5) Disclosure to qualifying foreign Government.

(A) It shall not constitute a violation of a protective order issued under section 2705 for a provider of electronic communication service to the public or remote computing service to disclose to the entity within a qualifying foreign government, designated in an executive agreement under section 2523, the fact of the existence of legal process issued under this section seeking the contents of a wire or electronic communication of a customer or subscriber who is a national or resident of the qualifying foreign government.

(B) Nothing in this paragraph shall be construed to modify or otherwise affect any other authority to make a motion to modify or quash a protective order issued under section 2705.