

2021

Not an Ocean Away, Only a Moment Away: A Prosecutor's Primer for Obtaining Remotely Stored Data

Robert J. Peters

Alicia D. Loy

Matthew Osteen

Joseph Remy

Justin Fitzsimmons

Follow this and additional works at: <https://open.mitchellhamline.edu/mhlr>

 Part of the [Evidence Commons](#), and the [Fourth Amendment Commons](#)

Recommended Citation

Peters, Robert J.; Loy, Alicia D.; Osteen, Matthew; Remy, Joseph; and Fitzsimmons, Justin (2021) "Not an Ocean Away, Only a Moment Away: A Prosecutor's Primer for Obtaining Remotely Stored Data," *Mitchell Hamline Law Review*: Vol. 47 : Iss. 3 , Article 6.

Available at: <https://open.mitchellhamline.edu/mhlr/vol47/iss3/6>

This Article is brought to you for free and open access by the Law Reviews and Journals at Mitchell Hamline Open Access. It has been accepted for inclusion in Mitchell Hamline Law Review by an authorized administrator of Mitchell Hamline Open Access. For more information, please contact sean.felhofer@mitchellhamline.edu.

© Mitchell Hamline School of Law

**NOT AN OCEAN AWAY, ONLY A MOMENT AWAY: A
PROSECUTOR'S PRIMER FOR OBTAINING
REMOTELY STORED DATA**

Robert J. Peters¹ Alicia D. Loy² Matthew Osteen³
Joseph Remy⁴ Justin Fitzsimmons⁵

¹ Robert J. Peters, Esq., is the senior attorney at Zero Abuse Project, where he develops and delivers state-of-the-art training and comprehensive technical assistance to prosecutors and child abuse multidisciplinary team members on crimes against children. Previously, Mr. Peters served as the senior cyber and economic crime attorney and general counsel with the National White Collar Crime Center (NW3C), as well as assistant prosecuting attorney and special prosecutor in various West Virginia jurisdictions. He specializes in the investigation and prosecution of sexual offenses and technology-facilitated child abuse and is founder and chair of the SHIELD Task Force, a 501(c)(3) child abuse awareness and prevention organization. Mr. Peters serves on the West Virginia Child Advocacy Network (WVCAN) Board of Directors and is a member of the West Virginia Center for Children's Justice. Mr. Peters' work on this project was supported by Award #2019-CI-FX-K006, awarded by the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice.

² Alicia D. Loy, Esq., is a cyber and economic crime attorney at the NW3C, where she assists in the development of curriculum for NW3C's judges and prosecutors courses, provides support for NW3C's prosecutorial technical assistance program, and develops content for webinars and podcasts on aspects of internet-facilitated crime. Ms. Loy graduated from West Virginia University College of Law with her Juris Doctor in May 2020, where she worked as a student attorney in the General Litigation Clinic and as an extern for the Honorable Michael John Aloia, Magistrate Judge for the Northern District of West Virginia.

³ Matthew Osteen is general counsel and cyber and economic crime attorney with the NW3C. He serves as a subject-matter expert on topics related to digital evidence, financial crime, intellectual property rights, and third-party data. Mr. Osteen also develops the curriculum for NW3C's judges and prosecutors courses.

⁴ Joseph Remy prosecuted a variety of criminal cases, including assault, bank fraud, network intrusions, and source code theft at the New York County (Manhattan) District Attorney's Office, where he became familiar with cybersecurity and digital forensics. As a certified cybercrime examiner (3CE) and certified blockchain expert (CBE), he joined the New Jersey Office of the Attorney General, where he investigated and prosecuted child exploitation offenses and cybercrimes while working on a number of legislative and policy matters. Mr. Remy is currently an assistant prosecutor in New Jersey and has served as an emergency medical technician since 2002.

⁵ Justin Fitzsimmons is an associate vice president at the NW3C. Justin oversees NW3C's prosecutorial and judicial programs and legal resources. In this position, he assists in the development and implementation of cyber, high-tech, and economic crime curriculum while providing training and technical assistance to law enforcement, prosecutors, and the judiciary across the nation. Before joining NW3C, Justin worked for SEARCH Group, Inc. as the director of High-Tech Training Services. Before SEARCH, Justin held the position of senior attorney with the National District Attorneys Association (NDAA). Within NDAA's National Center for Prosecution of Child Abuse (NCPA), he managed NCPA's technology-facilitated child sexual exploitation (TFCSE) unit, responding to requests for assistance in child sexual exploitation cases from prosecutors and law enforcement agencies across the United States. Previously, he served as an assistant state's attorney, prosecuting cases involving sexual exploitation and digital evidence. Currently, Justin is the president of the Board of Directors of the National Children's Alliance.

2021] NOT AN OCEAN AWAY, ONLY A MOMENT AWAY 1073

I. INTRODUCTION 1074

II. THE STORED COMMUNICATIONS ACT AND THE FOURTH AMENDMENT 1075

 A. *The Stored Communications Act*..... 1075

 B. *Problems with the Stored Communications Act* 1078

 C. *Fourth Amendment Implications and Stored Communications Act Trajectory* 1084

III. CLARIFYING LAWFUL OVERSEAS USE OF DATA ACT (CLOUD) ACT 1092

 A. *Access to Foreign Stored Data*..... 1092

 B. *Bilateral Agreements*..... 1093

IV. UNITED STATES—UNITED KINGDOM BILATERAL AGREEMENT..... 1095

 A. *Maintenance of Domestic Law*..... 1096

 B. *Proper Targeting*..... 1097

 C. *Issuance and Transmission of Orders*..... 1098

 D. *Production of Information* 1100

 E. *Minimization Procedures* 1100

 F. *Limitations on Use and Transfer*..... 1100

 G. *Compatibility and Non-Exclusivity* 1101

 H. *Expiry and Termination of the Agreement* 1101

V. HOW PROSECUTORS AND LAW ENFORCEMENT CAN OBTAIN REMOTELY STORED DATA..... 1102

 A. *Search Warrants and Digital Evidence*..... 1102

 B. *Obtaining Domestically Stored Data*..... 1104

 1. *Costs Associated with Obtaining the Data*..... 1110

 2. *How Should the Midgard Prosecutors Advise Officer Oss?*.. 1112

 C. *Obtaining Internationally Stored Data via CLOUD Act Agreement*..... 1113

 D. *Obtaining Internationally Stored Data via Mutual Legal Assistance Treaty (MLAT)* 1115

 1. *Can Officer Oss Access This Information in the Absence of a CLOUD Act Agreement?*..... 1115

 E. *Obtaining Internationally Stored Data Without MLATs or CLOUD Act Agreements*..... 1117

 1. *Does Officer Oss Have Any Legal Process Options in the Absence of Both Agreements?* 1117

 F. *Legal Implications of Extraterrestrial Data Storage*..... 1120

 1. *Can Officer Oss Access Joe Collector’s Data, Despite its Location in Outer Space?* 1122

VI. APPENDIX..... 1123

 A. *Long-Arm Statutes* 1123

Officer Kay Oss of the Midgard State Police received a report from a guidance counselor that a fourteen-year-old girl, Stacy, disclosed she was sexually abused by a forty-three-year-old man named John. Stacy told Officer Oss that John physically harmed her and took sexually explicit photos of her with his cell phone. Officer Oss is investigating John for various offenses he committed against Stacy. To support her investigation, Officer Oss wishes to obtain information from the cloud-based storage provider used by John, but she is uncertain whether she may obtain this information with a Midgard search warrant, as the servers used by the provider are located in Virginia.

I. INTRODUCTION

Digital evidence exists in almost every criminal case and provides unparalleled corroborative utility, particularly for crimes often committed in secret, such as child exploitation. This evidence is increasingly stored remotely on servers across state lines, around the globe, and beyond.⁶ It is therefore critical for prosecutors and law enforcement to develop an understanding of the pertinent domestic and international legal considerations for obtaining remotely stored data.

This Article provides an overview of the Stored Communications Act (SCA), the trajectory of Fourth Amendment jurisprudence since the SCA's passage, relevant provisions of the Clarifying Lawful Overseas Use of Data (CLOUD) Act, and bilateral agreements following the enactment of the CLOUD Act. This Article uses real-life scenarios that prosecutors and law enforcement face to explore the potential pitfalls of accessing remotely stored data and proposes possible solutions to those problems. Examples include practices for obtaining domestically stored data, obtaining internationally stored data via the CLOUD Act agreement or mutual legal assistance treaty (MLAT), obtaining internationally stored data in the absence of the CLOUD Act agreements or MLATs, and obtaining data stored in extraterrestrial locations.

⁶ Industry forecasters predict significant annual growth rates and increasing global cloud service revenue. See Louis Columbus, *Public Cloud Soaring to \$331B by 2022 According to Gartner*, FORBES (Apr. 7, 2019), <https://www.forbes.com/sites/louiscolumbus/2019/04/07/public-cloud-soaring-to-331b-by-2022-according-to-gartner/?sh=7b4726665739> [https://perma.cc/B526-2JU3]; see also *infra* Section V.F.

II. THE STORED COMMUNICATIONS ACT AND THE FOURTH AMENDMENT

A. *The Stored Communications Act*

The SCA “creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users’ private information.”⁷ Notably, Congress enacted the SCA in 1986, before many of today’s predominant technologies even existed.⁸ Disposable cameras were new arrivals to mainstream culture,⁹ but the World Wide Web¹⁰ and Nintendo Game Boy¹¹ would not debut for another three years. Given this cultural and technological context, it is unsurprising that the SCA’s provisions are often difficult for courts to reconcile with modern technology such as cloud-based data storage and complex anonymization platforms.

The SCA applies when law enforcement requests records or data about a customer from a communications service provider, rather than obtaining the same records from the customer’s own computer or device.¹² Prior to the enactment of the SCA, the third-party doctrine enabled law enforcement to obtain this data without violating the Fourth Amendment.

The United States Supreme Court created the third-party doctrine in the cases of *Smith*¹³ and *Miller*.¹⁴ The doctrine states that a person who voluntarily provides information to a third party relinquishes any reasonable expectation of privacy in that information, thus eliminating Fourth Amendment protection on that data.¹⁵ In *Smith*, the Court concluded that because the defendant voluntarily released dialed information to the telephone company and assumed the risk that such information could be revealed to the police, the defendant had no reasonable expectation of privacy in the numbers dialed from his

⁷ Rudolph J. Burshnic, *Applying the Stored Communications Act to the Civil Discovery of Social Networking Sites*, 69 WASH. & LEE L. REV. 1259, 1261–62 (2012) (quoting Orin S. Kerr, *A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1212 (2004)).

⁸ *Id.* at 1261.

⁹ Ernie Smith, *Point, Shoot, and Forget*, TEDIUM (July 26, 2018), <https://tedium.co/2018/07/26/disposable-camera-history/> [https://perma.cc/F8C2-MWAE].

¹⁰ *History of the Web*, WORLD WIDE WEB FOUND., <https://webfoundation.org/about/vision/history-of-the-web/> [https://perma.cc/8EZ5-5DL4].

¹¹ *Game Boy*, NAT’L MUSEUM AM. HIST., https://americanhistory.si.edu/collections/search/object/nmah_1253117 [https://perma.cc/5TZ7-ZYUL].

¹² Burshnic, *supra* note 9, at 1262.

¹³ *Smith v. Maryland*, 442 U.S. 735 (1979).

¹⁴ *United States v. Miller*, 425 U.S. 435 (1976).

¹⁵ *Id.* at 443.

telephone.¹⁶ In *Miller*, the Court held that the defendant's bank records, which showed the existence of the defendant's illegal whiskey enterprise, were voluntarily disclosed to the bank when the defendant made purchases.¹⁷ Because these records were voluntarily disclosed, the defendant

¹⁶ *Smith*, 442 U.S. at 745.

On March 5, 1976, in Baltimore, Md., Patricia McDonough was robbed. She gave the police a description of the robber and of a 1975 Monte Carlo automobile she had observed near the scene of the crime. . . . On March 16, police spotted a man who met McDonough's description driving a 1975 Monte Carlo in her neighborhood. By tracing the license plate number, police learned that the car was registered in the name of petitioner, Michael Lee Smith.

The next day, the telephone company, at police request, installed a pen register at its central offices to record the numbers dialed from the telephone at petitioner's home. The police did not get a warrant or court order before having the pen register installed. The register revealed that on March 17 a call was placed from petitioner's home to McDonough's phone. On the basis of this and other evidence, the police obtained a warrant to search petitioner's residence. . . .

Petitioner was indicted in the Criminal Court of Baltimore for robbery. By pretrial motion, he sought to suppress "all fruits derived from the pen register" on the ground that the police had failed to secure a warrant prior to its installation. The trial court denied the suppression motion, holding that the warrantless installation of the pen register did not violate the Fourth Amendment.

Id. at 737-38 (internal citations omitted).

¹⁷ *Miller*, 425 U.S. at 446.

On December 18, 1972, in response to an informant's tip, a deputy sheriff from Houston County, Ga., stopped a van-type truck occupied by two of respondent's alleged co-conspirators. The truck contained distillery apparatus and raw material. On January 9, 1973, a fire broke out in a . . . warehouse rented to respondent. During the blaze firemen and sheriff department officials discovered a 7,500-gallon-capacity distillery, 175 gallons of non-tax-paid whiskey, and related paraphernalia.

. . . [A]gents from the Treasury Department's Alcohol, Tobacco and Firearms Bureau presented grand jury subpoenas issued in blank by the clerk of the District Court, and completed by the United States Attorney's office, to the presidents of the [two banks], where respondent maintained accounts. The subpoenas required the two presidents to appear on January 24, 1973, and to produce

"all records of accounts, i.e., savings, checking, loan
or otherwise . . ."

The banks did not advise respondent that the subpoenas had been served but ordered their employees to make the records available and to provide copies of any documents the agents desired.

Id. at 437-38 (internal citations omitted).

Respondent was convicted of possessing an unregistered still, carrying on the business of a distiller without giving bond and with intent to defraud the Government of whiskey tax, possessing 175 gallons of

did not have a reasonable expectation of privacy to them.¹⁸ In recent years, the Court ruled that the third-party doctrine fails to justify government access to electronic communications made by a cell phone user and recorded by a cell phone provider under the Fourth Amendment.¹⁹

The SCA protects private customer data by creating different legal process levels based on the type of data sought by a government entity, which addresses Fourth Amendment privacy issues caused by the third-party doctrine.²⁰ The Act creates three categories of data: subscriber data (account holder name and address); transactional data (connectivity to account data); and content data (open and closed emails, group membership).²¹ The SCA designated both subscribers and transactional data as non-content.²² The three legal process levels created by the SCA correspond with the type of data being requested; more appreciable data requires a higher legal process.²³

Law enforcement may obtain subscriber data with a subpoena from a court of competent jurisdiction.²⁴ Data in this category includes basic subscriber information related to the customer's identity, the customer's relationship with the service provider, payment method, and basic connection records.²⁵ Transactional data includes information such as

whiskey upon which no taxes had been paid, and conspiring to defraud the United States of tax revenues. Prior to trial respondent moved to suppress copies of checks and other bank records obtained by means of allegedly defective subpoenas. . . .

The District Court overruled respondent's motion to suppress, and the evidence was admitted.

Id. at 436–37 (internal citations omitted).

¹⁸ *Id.* at 446 (“[W]e hold that respondent lacks the requisite Fourth Amendment interest to challenge the validity of the subpoenas.”).

¹⁹ *See* United States v. Jones, 565 U.S. 400 (2012); *see also* Carpenter v. United States, 138 S. Ct. 2206 (2018); Riley v. California, 573 U.S. 373, 403 (2014) (allowing the government access to cell-site records, which “hold for many Americans ‘the privacies of life,’ and contravenes any reasonable expectation of privacy in a person’s physical movements).

²⁰ Burshnic, *supra* note 9, at 1262–63.

²¹ DAVID W. HAGY, NAT’L INST. OF JUST., DIGITAL EVIDENCE IN THE COURTROOM: A GUIDE FOR LAW ENFORCEMENT AND PROSECUTORS 3 (2007).

²² *Id.*

²³ *Id.*

²⁴ *Id.* at 4.

²⁵ *Id.*; *see also* 18 U.S.C. § 2703 (2018).

A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

account activity logs, email addresses of the customer's correspondents, and friends lists; law enforcement may obtain this information with a court order under 18 U.S.C. § 2703(d) of the SCA.²⁶ This document is often referred to as a 2703(d) order, or a specific and articulable facts order.²⁷ This order may be issued by a federal magistrate or a district court with jurisdiction over the offense under investigation; state court judges authorized by state law may also issue 2703(d) orders.²⁸ The application for a 2703(d) order must provide "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation."²⁹ Finally, content data must be obtained with a search warrant based upon probable cause.³⁰ Data at this level includes everything in the account not considered either subscriber or transactional data, such as unopened communications (unread text messages or emails).³¹ Recently, case law added cell site location information (CSLI) to the category of content data requiring a warrant for law enforcement access.³²

B. *Problems with the Stored Communications Act*

As noted above, the SCA was enacted in an era without the advanced technology we know today. The SCA's drafters could not have anticipated the development of robust technology like the smartphone, which, as Justice Roberts noted in *Carpenter v. United States*, is now "almost a 'feature of human anatomy.'"³³ In this same vein, it is unlikely the SCA drafters could have predicted the global environment of data storage—and

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under [18 U.S.C. § 2703(c)(1) (2018)].

Id. § 2703(c)(2).

²⁶ See HAGY, *supra* note 23, at 4.

²⁷ See *id.*

²⁸ 18 U.S.C. § 2703(d) (2018).

²⁹ *Id.*

³⁰ HAGY, *supra* note 23, at 6.

³¹ *Id.*

³² *Id.*; see also *Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018) (holding that historical CSLI must be obtained with a search warrant rather than a § 2703(d) order).

³³ *Carpenter*, 138 S. Ct. at 2218 (quoting *Riley v. California*, 573 U.S. 373, 385 (2014)).

the jurisdictional issues that arise from that extensive system. Initially, the SCA only regulated data held within the territorial boundaries of the United States. The SCA created authority for law enforcement from one state to use the legal process to obtain stored communications on servers in a different state under a long-arm jurisdiction theory. With the exponential growth in technology use and data storage, many of today's communication companies stretch outside the United States.³⁴ For example, a United States communications company based in Washington state may host data on servers worldwide to meet international users' needs and data storage space requirements. Before amendment by the CLOUD Act, the SCA was silent regarding a US-based law enforcement officer's ability to access the same data on the company's server abroad.

Domestication of legal process was one of the jurisdictional difficulties the SCA sought to remedy. Before the SCA existed, local laws often mandated law enforcement to domesticate the legal process in either the company's state of incorporation or the state the data resided in. This arduous process often required the out-of-state law enforcement official to communicate with a local law enforcement agency. The out-of-state law enforcement officer would have to fill out an affidavit for the particular account or data sought and send the request to the local agency. The local agency then filled out the actual legal process and submitted it to the company. The company then responded with the relevant data to the local law enforcement agency, which had to forward it back to the out-of-state agency making the original request. The entire process embodied the age-old adage of a game of telephone.

Unfortunately, in trying to remedy the domestication issue, the SCA created an entirely different jurisdictional problem. Although the SCA is a federal statute, it relies on both the Federal Rules of Criminal Procedure for federal cases and the state level judicial process authorizing subpoenas, 2703(d) orders, and search warrants in state cases.³⁵ The SCA empowers a court of competent jurisdiction to issue a subpoena, court order, or a search warrant for the search and seizure of any information delineated in the Act.³⁶ A court of competent jurisdiction may be either a federal or state court, provided the court has jurisdiction over the offense.³⁷ The jurisdictional component of the SCA is broad to provide for the availability of multiple courts to issue warrants under the SCA.³⁸

³⁴ U.S. DEP'T OF JUST., PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT 10 (2019) [hereinafter THE PURPOSE AND IMPACT OF THE CLOUD ACT].

³⁵ 18 U.S.C. § 2703(e)(1)(A) (2018).

³⁶ *Id.* § 2703(d).

³⁷ *Id.*

³⁸ *Id.* In a federal context, a "court of competent jurisdiction" is defined in relevant part as:

The SCA's specific jurisdictional issue emerges when a state judge issues legal process under the auspices of the SCA's authority for digital data stored outside of the territorial boundary of the issuing state. Importantly, a court of competent jurisdiction includes "a court of general criminal jurisdiction *of a State* authorized by the law of that State to issue search warrants."³⁹ As noted in the legislative history for the initial enactment of the SCA and its subsequent amendments via the PATRIOT Act, Congress intended the authority granted by the SCA to issue warrants for stored communications to be broad in application to accommodate expanding technologies.⁴⁰ One court acknowledged that the general authority of a state court to issue warrants is sufficient; specific authority to issue warrants in cases of stored communications is not required.⁴¹ A prior version of § 2703(a) stated:

-
- (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that—
- (i) has jurisdiction over the offense being investigated; [or]
 - (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or
 - (iii) is acting on a request for foreign assistance.

Id. § 2711(3)(A)(i)–(iii). The last jurisdictional provision, whereby a federal judge may issue a warrant when acting on a request for foreign assistance, is distinct from authority granted by the CLOUD Act. This jurisdictional provision specifically refers to 18 U.S.C. § 3512 (2018), which grants federal judges authority to respond to: foreign requests for assistance in criminal investigations and prosecutions by issuing search warrants; issue warrants under § 2703 for stored wire or electronic communications; file orders for pen registers or trap and trace devices; or serve subpoenas for testimony or production of documents. 18 U.S.C. § 3512 (2018). The provision in § 2711(3)(A)(iii) clarifies that a court acting with jurisdictional authority under § 3512 is also considered to be a court of competent jurisdiction for purposes of issuing warrants, subpoenas, and orders under the SCA. This statutory definition provides three ways in which a federal court may qualify as a court of competent jurisdiction for purposes of the SCA, which are joined by the word "or." This conjunction indicates that the court issuing the warrant does not necessarily have to be located within the same jurisdiction as the location where the electronic communications, records, or other information are stored. Any federal district court, federal magistrate judge, or United States appellate court that meets the court of competent jurisdiction definition may issue a warrant, subpoena, or court order for information protected by the SCA. *See generally* Hubbard v. MySpace, Inc., 788 F. Supp. 2d 319, 323–24 (S.D.N.Y. 2011).

³⁹ 18 U.S.C. § 2711(3)(B) (2018) (emphasis added).

⁴⁰ 132 CONG. REC. 14,886 (1986) (statement of Rep. Kastenmeier) ("[L]egislation which protects electronic communications from interceptions by either private parties or the Government should be comprehensive, and not limited to particular types or techniques of communicating."); *see also* United States v. Councilman, 418 F.3d 67, 79 (1st Cir. 2005) (en banc) (concluding "that the term 'electronic communication' includes transient electronic storage that is intrinsic to the communication process for such communications.").

⁴¹ *Hubbard*, 788 F. Supp. 2d at 323–24.

A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation *or an equivalent State warrant*.⁴²

Thus, a state court could have the authority to issue a warrant by either having jurisdiction over the offense being investigated or by being in the district where the stored communications are located.

State authority to issue warrants under the SCA is identical to the federal authority, though additional process might be required to ensure a warrant's validity if issued by the state court judge.⁴³ The U.S. District Court for the Southern District of New York in the case of *Hubbard v. Myspace*,

On December 1, 2007, Georgia authorities arrested plaintiff for contributing to the delinquency of a minor and “enticing a child for indecent purposes.” On January 29, 2008, in the course of investigating plaintiff’s alleged crimes, the sheriff’s office of Cherokee County, Georgia, obtained a search warrant from the Magistrate Court of Cherokee County. The warrant instructed “all peace officers of the state of Georgia” to search MySpace’s custodian of records in Beverly Hills, California, for:

“Records concerning the identity of the user with the Friend ID 79001021 consisting of name, postal code, country, e-mail address, date of account creation, IP address at account sign-up, logs showing IP address and date stamps for account accesses, and the contents of any private messages in the user’s inbox and sent mail folders.”

That same day, the sheriff’s office faxed the warrant to MySpace’s custodian of records in California. MySpace subsequently “accessed and produced and disclosed the requested personal and private user information, data, records and/or the contents of electronic communications to law enforcement.”

Id. at 321. Hubbard ultimately entered a guilty plea but later sued Myspace, alleging that “MySpace’s disclosure of records and information pertaining to his account violated the Stored Communications Act. . . .” *Id.* The *Hubbard* court noted that extraterritorial warrants are permissible under 18 U.S.C. § 2703(a) and dismissed the complaint. *Id.* at 325–26.

⁴² 18 U.S.C. § 2703(a) (2009) (emphasis added).

⁴³ See *Hubbard*, 788 F. Supp. 2d. at 325. While *Hubbard* states “Section 2703(a) does not impermissibly expand the power of Georgia magistrates or any other courts,” the court’s analysis seems to suggest that, if the warrant issued by the state magistrate conforms to the requirements of a SCA warrant issued by a federal magistrate, then the warrant will be enforceable so long as the state has a long-arm statute allowing for extraterritorial applicability, as Georgia did in this case. *Id.* at 326.

Inc., focusing on the “equivalent State warrant” portion of this statute, held that the qualifications of a federal court to be a court of competent jurisdiction were implicitly applied to the qualifications of a state court.⁴⁴ The *Hubbard* court interpreted the “jurisdiction over the offense under investigation” provision to require only that the judge has the authority to issue a warrant for the investigation; there is no requirement for the issuing judge to have the jurisdiction to preside over a trial for the suspect for whom the warrant is issued.⁴⁵ The court found that by passing the SCA, Congress “specifically intended to allow federal courts to authorize searches beyond their normal territorial jurisdictions,”⁴⁶ and if this is true of federal courts, “the same ought to be true of equivalent state warrants.”⁴⁷ *Hubbard* further noted that Georgia law “appears to recognize the heightened territorial authority that magistrates and judges may have in issuing [SCA] warrants.”⁴⁸

Congress clearly intended for warrants issued under the SCA by a court of competent jurisdiction to extend beyond territorial jurisdiction; as the *Ackies*⁴⁹ court articulated, the SCA empowered courts to “permit searches . . . beyond the courts’ usual geographic jurisdictions.”⁵⁰ The House Report clarified this point in 2001 when the PATRIOT Act, which amended the SCA in part, passed:

An investigator, for example, located in Boston who is investigating a suspected terrorist in that city, might have to seek a suspect’s electronic e-mail from an Internet service

⁴⁴ *Id.*

⁴⁵ *Id.* at 324.

⁴⁶ *Id.* at 325.

⁴⁷ *Id.* at 326.

⁴⁸ *Id.* While this case was heard in the Southern District of New York, the search warrant at issue (which plaintiff claimed violated the SCA) was issued by a state magistrate in Georgia, authorizing “all peace officers of the state of Georgia” to search MySpace records relevant to the plaintiff’s alleged offenses under a Georgia law that criminalized “contributing to the delinquency of a minor and ‘enticing a child for indecent purposes.’” *Id.* at 321. MySpace, a company located in California, had a choice of forum provision within its Terms of Use Agreement, making New York the appropriate forum. Class Action Complaint at 3, *Hubbard v. MySpace, Inc.*, 788 F. Supp. 2d 319 (S.D.N.Y. 2011) (No. 11-CV-0433).

⁴⁹ *United States v. Ackies*, 918 F.3d 190, 202 (1st Cir. 2019). “Law enforcement began investigating Ackies in the fall of 2015, beginning with information from a cooperating witness who became a cooperating defendant . . . concerning his drug trafficking with a man he knew then as ‘Boyd’ (determined at trial to be Ackies).” *Id.* at 195. Investigators obtained precise location information (PLI) “from a magistrate judge in Maine pursuant to a provision of the SCA, 18 U.S.C. § 2703, and Fed. R. Crim. P. 41 (‘Rule 41’) for two cell phones.” *Id.* “Ackies was arrested . . . and charged in February 2016 with violations of 21 U.S.C. §§ 846 and 841(a)(1), conspiracy to possess and possession with intent to distribute heroin and cocaine base.” *Id.* The defendant moved to suppress the PLI warrants on several grounds, but the First Circuit rejected the defendant’s attempt to apply Rule 41(b) of the Federal Rules of Criminal Procedure to limit the jurisdiction conferred by the SCA. *Id.* at 201–03.

⁵⁰ *Id.* at 202.

provide[r] (ISP) account located in California. The investigator would then need to coordinate with agents, prosecutors and judges in the district in California where the ISP is located to obtain a warrant to search [The Act] amends § 2703 to authorize the court with jurisdiction over the investigation to issue the warrant directly.⁵¹

Further, the text of § 2711 clarifies that “the term ‘court of competent jurisdiction’ includes . . . a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants.”⁵² One court acknowledged that the word “includes” was originally the word “means” prior to the 2009 amendment to the SCA; by using the word “includes,” Congress intended to expand the definition of “court of competent jurisdiction.”⁵³ This same court acknowledged that each state may have differing procedures and laws regarding the operation of the state court system.⁵⁴ To avoid this problem, Congress used broad language to create a statute that allows for the authorization of many types of state courts to issue warrants under the SCA, provided that the court has general criminal jurisdiction.⁵⁵

The only remaining jurisdictional hurdle to clear, if any, is posed by a state’s constitution or long-arm statute.⁵⁶ In the absence of any clear prohibition by state law, the SCA confers jurisdiction to state courts in this

⁵¹ *Id.* (citing H.R. REP. NO. 107-236, pt. 1, at 57 (2001)); see also *In re Yahoo, Inc.*, No. 07-3194-MB, 2007 U.S. Dist. LEXIS 37601 (D. Ariz. May 21, 2007) (finding that Congress intended for district courts to have the authority under the Electronic Communications Privacy Act to obtain electronically-stored communications from other jurisdictions).

⁵² 18 U.S.C. § 2711(3)(B) (2018).

⁵³ *John K. MacIver Inst. for Pub. Pol’y, Inc. v. Schmitz*, 243 F.Supp.3d 1028, 1033 (W.D. Wis. 2017). “In this civil action, The John K. MacIver Institute for Public Policy, Inc., purports to assert class claims against various state actors, alleging that they violated the [SCA] . . . by seizing electronic information pursuant to search warrants issued by a County Circuit Court Judge during the course of a Wisconsin . . . proceeding.” *Id.* at 1030. The defendants moved to dismiss, in part based on SCA statutory defenses. The court granted the motions to dismiss, finding no SCA violation since the warrants in question were issued by a court of competent jurisdiction. *Id.* at 1032-35. Among other arguments for a broader interpretation of SCA jurisdiction, the court noted that “the SCA specifically makes valid warrants issued by federal magistrate judges[, which] further suggests that Congress did not intend to exclusively limit those [SCA-conferred] powers to judges who can enter felony judgments.” *Id.* at 1034.

⁵⁴ *Id.*

⁵⁵ *Id.*

⁵⁶ See *infra* Part VI (listing state long-arm statutes and related case law); see also *Long-Arm Statutes: A Fifty-State Survey*, VEDDER PRICE (2003), <http://euro.ecom.cmu.edu/program/law/08-732/Jurisdiction/LongArmSurvey.pdf> [<https://perma.cc/32WS-GZDJ>].

context;⁵⁷ SCA warrants are not limited to the territorial jurisdiction of the issuing authority.⁵⁸ This “promote[s] prosecutorial and judicial efficiency by permitting courts in locus of crime to preside over both investigation and adjudication,” and also relieves the burden on courts in jurisdictions that host larger internet-service providers.⁵⁹

C. *Fourth Amendment Implications and Stored Communications Act Trajectory*

As mentioned previously, the third-party doctrine and the SCA are less than perfect means for handling today’s technology which, when considering the collective data from these powerful devices, paints a near-perfect picture of individuals’ daily lives. This picture is much more intimate than a thermal imaging device,⁶⁰ disclosing “at what hour each night the lady

⁵⁷ See *State v. Esarey*, 67 A.3d 1001, 1008 n.17 (Conn. 2013) (“Indeed, there is nothing in the language of § 54-33a, our search warrant statute, that expressly restricts a trial judge’s authority to order searches to Connecticut’s borders. . . . Thus, consistent with the Stored Communications Act, 18 U.S.C. § 2703(b), it would appear to us that, under our existing statutes, a Connecticut trial judge may, in connection with the investigation of a crime committed here, order a search of electronically stored communications contained on a remote computing service’s server located in another state . . .”).

⁵⁸ *Hubbard v. MySpace, Inc.*, 788 F.Supp.2d 319, 325 (S.D.N.Y. 2011).

⁵⁹ *Esarey*, 67 A.3d at 1008 (analyzing *In re Yahoo, Inc.*, No. 07-3194-MB, 2007 U.S. Dist. LEXIS 37601 (D. Ariz. May 21, 2007)). Commentators have opined that certain Patriot Act amendments were designed “to shift the responsibility for issuance” of search warrants from courts where service providers are located “to the court with jurisdiction over the offense being investigated,” since prior to the Patriot Act, “a disproportionate number of such orders were issued in the Eastern District of Virginia, where AOL is located.” Patricia L. Bellia, *Surveillance Law Through Cyberlaw’s Lens*, 72 GEO. WASH. L. REV. 1375, 1454 (Aug. 2004). This was also calculated to reduce the unnecessary costs, which accompany domestication of search warrants. Paul K. Ohm, *Parallel Effect Statutes and E-mail “Warrants”: Reframing the Internet Surveillance Debate*, 72 GEO. WASH. L. REV. 1599, 1614–15, n.80 (Aug. 2004) (citing H.R. REP. NO. 107-236, pt. 1, at 57 (2001)).

⁶⁰ The *Kyllo* Court determined whether use of a thermal-imaging device aimed at a private residence was considered a “search” within the meaning of the Fourth Amendment.

In 1991 Agent William Elliott of the United States Department of the Interior came to suspect that marijuana was being grown in the home belonging to petitioner Danny Kyllo. . . . Indoor marijuana growth typically requires high-intensity lamps. In order to determine whether an amount of heat was emanating from petitioner’s home consistent with the use of such lamps, at 3:20 a.m. on January 16, 1992, Agent Elliott and Dan Haas used an Agema Thermovision 210 thermal imager to scan the triplex. Thermal imagers detect infrared radiation, which virtually all objects emit but which is not visible to the naked eye. The imager converts radiation into images based on relative warmth – black is cool, white is hot, shades of gray connote relative differences; in that respect, it operates somewhat like a video camera showing heat images. The scan of Kyllo’s home took only a few minutes and was performed

of the house takes her daily sauna and bath,”⁶¹ and infinitely more comprehensive of a person’s daily movements than could ever be obtained through a law enforcement officer’s personal observation of an individual’s movements on the street.

The Supreme Court has recognized, even if it has not directly confronted, the Fourth Amendment privacy issues created by the SCA and the third-party doctrine. The Court seems to favor a reasonable expectation of privacy approach, which may take the form of a pattern of life analysis and mosaic theory approach. This Section discusses the Supreme Court’s present views on the third-party doctrine and predicts how the Court may handle future challenges to the SCA on Fourth Amendment grounds.

The Court has maintained that the third-party doctrine, as applied to content protected under the SCA, is still good law; however, in recent years, the Court has noted that digital data stored on a device and sent to servers belonging to cell phone providers may require more protection, but it has not overturned *Smith* or *Miller*.⁶² Two major concepts are relevant for discussing a broad means of protection for potentially revealing digital data rather than the “one size fits all” approach currently present in the third-party doctrine. These concepts are known as the mosaic theory and pattern of life analysis and, while distinct, discussion of one necessarily requires discussion of the other in the same context.

The idea behind the mosaic theory⁶³ is that a long-term, large-scale data collection effort may reveal details about an individual that a single

from the passenger seat of Agent Elliott’s vehicle across the street from the front of the house and also from the street in back of the house. The scan showed that the roof over the garage and a side wall of petitioner’s home were relatively hot compared to the rest of the home and substantially warmer than neighboring homes in the triplex. Agent Elliott concluded that petitioner was using halide lights to grow marijuana in his house, which indeed he was. Based on tips from informants, utility bills, and the thermal imaging, a Federal Magistrate Judge issued a warrant authorizing a search of petitioner’s home, and the agents found an indoor growing operation involving more than 100 plants.

Kyllo v. United States, 533 U.S. 27, 29–30 (2001) (holding that the thermal imaging constituted an unlawful search).

⁶¹ *Id.* at 38.

⁶² See *United States v. Jones*, 565 U.S. 400 (2012) (finding that attachment of a GPS device to a vehicle and surveillance of vehicle’s movements on public streets was a “search” within the Fourth Amendment); *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (finding government surveillance of an individual’s physical movements captured through CSLI was considered a “search”); see also *Riley v. California*, 573 U.S. 373 (2014) (holding interest in protecting officers’ safety and preventing destruction of evidence did not justify dispensing with warrant requirements for searches of cell phone data).

⁶³ Cultural anthropology and financial investment analysis both use the term “mosaic theory.” Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012). In a legal context, the term was first coined by the U.S. Court of Appeals for the

observation could not reveal.⁶⁴ A mosaic is composed of hundreds or thousands of pieces of glass; looking at each piece individually, one cannot discern much. When those pieces of glass are arranged in a particular way, one may step back and look at the pieces of glass to see the beautiful image that is formed. Likewise, different digital data pieces may be gathered from various sources that do not reveal much about the user, but when put together, a larger picture of the person's daily life may form. Putting the pieces together forms the mosaic; adding more pieces forms an even larger mosaic. Stepping back and looking at the whole mosaic to see something much more than the sum of its parts is the pattern of life analysis.

The pattern of life analysis refers to figuring out the normal habits of a person's life—both public and private.⁶⁵ Traditional law enforcement and intelligence techniques can establish a pattern of life for a particular person; however, technology allows law enforcement to establish a pattern of life in a more comprehensive manner. This can be done through examining the digital evidence on a smartphone—call logs, GPS coordinates, time-stamped photos⁶⁶—or any number of other digital devices, from wearable health monitors to home assistants to smart vehicles.

For example, a law enforcement officer working the beat may see an individual enter a gym at nine o'clock on a Tuesday morning, but the officer may not know what the individual does after leaving the gym unless the officer followed him. This type of investigation requires time, personnel, and documentation. If the same officer wished to track the same individual's movements by using the GPS data from the individual's cell phone, then the officer would have an even more comprehensive picture of the individual's whereabouts than if the officer followed the individual.

Each individual GPS data point (the pieces of glass in the mosaic analogy) places the individual at a particular location at a particular time. The officer, with very little effort other than requesting the information from the cell phone provider, will be able to see that individual's pattern of life. The officer may note that the individual goes to the gym four days a week, works in an office building downtown, and visits the Protestant church once a week. These details, while seemingly innocent on the surface, may prove to reveal much more personal information that an individual may not wish to disclose to anyone—let alone law enforcement—such as the individual's religious or political affiliations or sexual practices.

District of Columbia Circuit in *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), an underpinning of *Jones*. *Id.*

⁶⁴ Paul Rozenzweig, *In Defense of the Mosaic Theory*, LAWFARE (Nov. 29, 2017), <https://www.lawfareblog.com/defense-mosaic-theory> [https://perma.cc/VMZ9-NLXY].

⁶⁵ *Id.*

⁶⁶ *Id.*

The Supreme Court has shifted away from strict application of the third-party doctrine to analyzing the type of data collected, the amount of data collected, and the time period represented by the data.⁶⁷ This shift began in *United States v. Jones*, which was decided on other grounds, but Justice Sotomayor criticized the third-party doctrine in a separate concurring opinion.⁶⁸ Justice Sotomayor noted that the Court should revisit the third-party doctrine, stating,

This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence *ceases to treat secrecy as a prerequisite for privacy*.⁶⁹

In its continued reexamination of digital data, the Court in *Riley v. California*⁷⁰ held that the Fourth Amendment prohibited a warrantless

⁶⁷ See *Carpenter*, 138 S. Ct. 2206; *Riley*, 573 U.S. at 37.

⁶⁸ *United States v. Jones*, 565 U.S. 400, 430 (2012). In *Jones*, the government placed a tracking device on the undercarriage of the defendant's wife's car, and the government tracked the car (used by the defendant for drug operations) over the course of four weeks. *Id.* at 403. Justice Scalia, writing for the majority, seemed to resurrect the long-dead trespass analysis for determining whether a search under the Fourth Amendment has occurred. *Id.* at 404-12. Justice Alito noted in concurrence that trespass is unnecessary for many forms of surveillance. *Id.* at 429-31 (Alito, J., concurring). Justice Sotomayor, elaborating on Justice Alito's comment, noted the reasonable expectation of privacy test, as established in *Katz v. United States*, augmented the trespass test, meaning trespass is sufficient (but not necessary) to find a search took place. *Id.* at 414-16 (Sotomayor, J., concurring) (citing *Katz v. United States*, 389 U.S. 347, 361 (1967)). This is particularly important in today's age with electronically stored data, and Justice Sotomayor discusses the dangers of relying on the majority's opinion and the trespass analysis alone since there can be no physical trespass of digital data. *Id.* at 417-18.

⁶⁹ *Id.* (emphasis added).

⁷⁰ 573 U.S. 373 (2014).

David Riley was stopped by a police officer for driving with expired registration tags. In the course of the stop, the officer also learned that Riley's license had been suspended. The officer impounded Riley's car, pursuant to department policy, and another officer conducted an inventory search of the car. Riley was arrested for possession of concealed and loaded firearms when that search turned up two handguns under the car's hood.

An officer searched Riley incident to the arrest and found items associated with the "Bloods" street gang. He also seized a cell phone from Riley's pants pocket. According to Riley's uncontradicted assertion, the phone was a "smart phone," a cell phone with a broad

search of a cell phone, on the grounds that a cell phone does not pose a risk to officer safety to justify a search of the phone's contents incident to its owner's arrest. The Court noted the cell phones' immense storage capacity and that the data stored on a cell phone can provide a means of reconstructing a person's private life.⁷¹

The Court in *Riley* did not create a separate standard for digital data, yet the Court acknowledged the importance of cell phones in today's society, which helped form the Supreme Court's future analysis. *Carpenter v. United States* held that cell site location information (CSLI) cannot be obtained from cellular service providers by law enforcement without a warrant.⁷² Justice Roberts, writing for the majority, decided that CSLI deserves heightened protection due to the data's revealing nature, and society would not reasonably expect law enforcement to be able to monitor and document every individual's movement with near-perfect precision.⁷³ The Court did not explicitly overrule *Smith* or *Miller* to invalidate the third-party doctrine; *Carpenter* merely works within the confines of the third-party doctrine and creates an exception for CSLI. Justice Alito criticized the Court's decision for being entirely unprecedented.⁷⁴

Because the Court is beginning to question the third-party doctrine's utility in today's digital world, prosecutors should be prepared for the different avenues of legal process to undergo change or become more

range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity. The officer accessed information on the phone and noticed that some words (presumably in text messages or a contacts list) were preceded by the letters "CK"—a label that, he believed, stood for "Crip Killers," a slang term for members of the Bloods gang.

At the police station about two hours after the arrest, a detective specializing in gangs further examined the contents of the phone. The detective testified that he "went through" Riley's phone "looking for evidence." . . . The police also found photographs of Riley standing in front of a car they suspected had been involved in a shooting a few weeks earlier.

Riley was ultimately charged, in connection with that earlier shooting, with firing at an occupied vehicle, assault with a semiautomatic firearm, and attempted murder. . . . Prior to trial, Riley moved to suppress all evidence that the police had obtained from his cell phone. He contended that the searches of his phone violated the Fourth Amendment, because they had been performed without a warrant and were not otherwise justified by exigent circumstances. The trial court rejected that argument.

Id. at 378–79 (internal citations omitted).

⁷¹ *Id.* at 394.

⁷² 138 S. Ct. 2206 (2018).

⁷³ *Id.* at 2218.

⁷⁴ *Id.* at 2247.

stringent. It appears that, based on the cases discussed above and the Justices' opinions on privacy protections for digital data, the Court may be heading in the direction of adopting a pattern of life and mosaic theory analysis. An alternative trajectory may focus on a strict review of search warrant affidavits, comparing the specific facts of the affidavit's probable cause section to determine whether each category of data requested for search and seizure is supported by probable cause and particularity for that discrete data type. In support of this trend, boilerplate search warrants for "all" the data on a device, or in an account, are being routinely rejected, or in the alternative, courts highlight the specific facts supporting unique data types and indicating that only those specific categories could be searched.⁷⁵

The Justices seem to favor emphasis of privacy concerns over the traditional third-party doctrine because when the third-party doctrine was created, the technology available to the general public was much more simplistic, and the third-party doctrine is impractical considering the sheer volume of revealing, personal data that is collected from individuals' devices every second. From this discussion, it is the authors' opinion that, if practicable, law enforcement officers should always obtain a warrant for the contents of communications, even if that data may otherwise be obtained through a 2703(d) order or subpoena.

Beyond the Supreme Court opinions, state courts and legislatures are also emphasizing privacy over the traditional third-party doctrine. In the 2020 election, Michigan voters took a dramatic step and approved an amendment to the state constitution which expanded warrant requirements to include electronic data and electronic communications.⁷⁶ As amended, the Michigan Constitution requires a warrant for the government "to access electronic data or electronic communication."⁷⁷ It is unclear if the

⁷⁵ "[S]eparate probable cause is required to search each of the categories of information found on the cellphones." *United States v. Morton*, 984 F.3d 421, 425 (5th Cir. 2021). "[T]he November 12th Warrant did not seek any and all data or digital information; instead, it sought only five enumerated categories of digital information. The November 12th Warrant did not contain language that would suggest an impermissibly broad scope such as 'any and all' or 'including but not limited to.' The categories limited the search to call logs, subscriber information, and various forms of messaging. The November 12th Warrant described what the officers believed would be found on the phone with specificity [to the text of the note] and thereby satisfied an important metric in judging particularity. Further, the November 12th Warrant was limited to a three-day period around the shooting, unlike the warrants in *Wheeler* and *Buckham* that lacked any temporal limitations." *State v. Wilson*, No. 1904007242, 2021 Del. Super. LEXIS 84, at *15 (Del. Super. Ct. Jan. 29, 2021).

⁷⁶ See Lester Graham, *Election 2020: Michigan Voters Approve Proposal 2, Protecting Electronic Data*, MICH. RADIO (Nov. 4, 2020), <https://www.michiganradio.org/post/election-2020-michigan-voters-approve-proposal-2-protecting-electronic-data> [<https://perma.cc/6SDT-9SQV>].

⁷⁷ *Id.* Proposal 2 amended Article 1, Section 11 of the Michigan Constitution to read as follows:

amendment refers only to data stored locally or if the amendment covers data stored by service providers. If the latter holds true, Michigan has effectively eliminated the third-party doctrine when applied to electronic data and communications.

In some states without codified exceptions to the third-party doctrine for electronic data and communications, state courts have stepped in to provide such exceptions, and in some cases, eliminated the third-party doctrine altogether.⁷⁸ A recent outlier decision from Arizona, *State v. Mixton*,⁷⁹ saw the court decline to apply the third-party doctrine in a case involving a defendant's IP address. There, the court found a reasonable expectation of privacy in one's IP address and required a search warrant to obtain one's IP address, in direct conflict with numerous jurisdictions.⁸⁰

The person, houses, papers, ~~and~~ possessions, **electronic data, and electronic communications** of every person shall be secure from unreasonable searches and seizures. No warrant to search any place or to seize any person or things or **to access electronic data or electronic communications** shall issue without describing them, nor without probable cause, supported by oath or affirmation. . . .

Statewide Ballot Proposal 20-2: Protection of Electronic Data and Communications, CITIZENS RSCH. COUNCIL MICHIGAN (Oct. 2020), https://crcmich.org/wp-content/uploads/Memo1164-Proposal_2_Search_and_seizure_of_electronic_data.pdf [<https://perma.cc/XWL3-UJSF>].

⁷⁸ See, e.g., *People v. Chapman*, 679 P.2d 62, 67 n.6 (Cal. 1984) (rejecting the "fiction" in *Miller* and *Smith* that a person has no reasonable expectation of privacy in bank or phone call records); *People v. Sporleder*, 666 P.2d 135, 141-42 (Colo. 1983) (rejecting *Smith* and finding reasonable expectation of privacy in phone numbers dialed); *Charnes v. DiGiacomo*, 612 P.2d 1117, 1120-21 (Colo. 1980) (rejecting *Miller* in construing state constitution's search-and-seizure provisions); *Shaktman v. State*, 553 So. 2d 148, 151 (Fla. 1989) (replicating the finding in *Sporleder*); *State v. Walton*, 324 P.3d 876, 906 (Haw. 2014) (indicating that *Miller* and *Smith* "incorrectly rely on the principle that individuals who convey information to a third party have assumed the risk of that party disclosing the information to the government. In our times individuals may have no reasonable alternative"); *State v. Thompson*, 760 P.2d 1162, 1165 (Idaho 1988) (finding that "in Idaho there is a legitimate and reasonable expectation of privacy in the phone numbers that are dialed."); *People v. DeLaire*, 610 N.E.2d 1277, 1282 (Ill. App. Ct. 1993) (describing how "[the court] believe[s] that citizens have a legitimate expectation that their telephone records will not be disclosed"); *Commonwealth v. DeJohn*, 403 A.2d 1283, 1289 (Pa. 1979) ("As we believe that *Miller* establishes a dangerous precedent, with great potential for abuse, we decline to follow that case when construing the state constitutional protection against unreasonable searches and seizures."); *State v. Thompson*, 810 P.2d 415, 418 (Utah 1991) (rejecting *Miller*).

⁷⁹ 447 P.3d 829 (Ariz. Ct. App. 2019).

⁸⁰ See, e.g., *Hatcher v. State*, 726 S.E.2d 117, 120 (Ga. Ct. App. 2012) ("[W]e doubt that an Internet service subscriber can have a reasonable expectation of privacy in the subscriber information that he voluntarily conveys to an Internet service provider in order to obtain Internet service."); *State v. Baric*, 919 N.W.2d 221, 228 (Wis. Ct. App. 2018) ("Baric has not shown by a preponderance of the evidence that he had a reasonable expectation of privacy in . . . his IP address."); *State v. Lemasters*, No. CA2012-12-028, 2013 Ohio App. LEXIS 3009, at *12 (Ohio Ct. App. July 8, 2013) ("Lemaster's Fourth Amendment rights

The *Mixton* court looked to New Jersey for support in finding a reasonable expectation of privacy in IP addresses⁸¹ but failed to acknowledge that New Jersey allows law enforcement to obtain IP addresses with a subpoena.⁸² The decision relies heavily on New Jersey as an example of a growing trend toward expansions of privacy outweighing law enforcement interests in investigating crimes. While the rationale of the *Mixton* court was incorrect and ultimately corrected by the Arizona Supreme Court,⁸³ both the trajectory of privacy-oriented jurisprudence and the wisdom of obtaining search warrants when practicable, are undeniable.

were not implicated by Detective Penwell's use of the file-sharing system, or in his obtaining Lemasters' information from Time Warner based upon Lemaster's IP address."); *State v. Rodriguez*, No. P2-2014-3011A, 2017 R.I. Super. LEXIS 89, at *28 (R.I. Super. Ct. May 30, 2017) ("Defendant has not established either a subjectively or objectively reasonable expectation of privacy in the subscriber information held by Verizon."); *State v. Mello*, 27 A.3d 771 (2011) (finding individuals have no expectation of privacy in non-content data shared with a service provider); *Commonwealth v. Do*, 86 Va. Cir. 483 (Cir. Ct. 2013) (finding that a defendant's subjective intent to hide his IP address does not create a reasonable expectation of privacy); *State v. Leblanc*, 137 So. 3d 656, 662 (La. Ct. App. 2014) ("[W]here an internet subscriber voluntarily discloses routine billing information to an ISP in order to receive service, he has no reasonable expectation of privacy in that information, and, therefore, the issuance of a search warrant for its disclosure would not be required."); *State v. Peppin*, 347 P.3d 906 (Wash. Ct. App. 2015) (holding there is no reasonable expectation of privacy in data exposed publicly); *State v. Roberts*, 345 P.3d 1226, 1236 (Utah 2015) (noting "the overwhelming weight of authority finding no reasonable expectation of privacy in subscription information, like an IP address, given to an internet service provider").

⁸¹ *See State v. Reid*, 945 A.2d 26, 33 (N.J. 2008) (noting that internet users are "entitled to expect confidentiality" in this information, and the fact that they have disclosed their identities to third party internet service providers "does not upend the privacy interest at stake").

⁸² *See id.* at 36 (explaining that a finding of a reasonable expectation of privacy under the state constitution does not necessarily trigger a warrant requirement and that a grand jury subpoena satisfies the requirements of the New Jersey Constitution as long as the data "bear some possible relationship[, however indirect,] to the grand jury investigation" (citing *State v. Mcallister*, 875 A.2d 866, 876 (N.J. 2005))).

⁸³ *See State v. Mixton*, 478 P.3d 1227, 1229 (Ariz. 2021) (holding that search warrants and court orders are not required to obtain IP addresses and other ISP subscriber information and that an administrative subpoena is sufficient). The Arizona Supreme Court noted that an expectation of privacy in this "non-content information is unreasonable in light of the nature of the information; it is voluntarily shared with third parties; and such third parties own, and often engage in pervasive legal derivative use" of the information. *Id.* at 1240.

III. CLARIFYING LAWFUL OVERSEAS USE OF DATA ACT (CLOUD) ACT⁸⁴

The CLOUD Act aims to combat the recent influx of data requests to US-based global providers from abroad in a manner that protects user privacy and civil liberties.⁸⁵ The CLOUD Act amends the SCA to include an affirmative statement that the SCA covers data stored on servers located outside the United States. The CLOUD Act contains two central parts: (1) the provision for access to foreign stored data and (2) the authorization of bilateral executive agreements to facilitate sharing data held by entities within the United States with law enforcement in foreign sovereign jurisdictions.⁸⁶

A. Access to Foreign Stored Data

First, the CLOUD Act facilitates access to electronic information, even if it is stored overseas, for law enforcement investigations.⁸⁷ Data covered by the CLOUD Act is the same data covered by the other SCA provisions, namely, “contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber.”⁸⁸ The data sought must be in a United States corporation’s, organization’s, or legal person’s possession or control.⁸⁹ When law enforcement successfully obtains a warrant to access data protected by the SCA and stored abroad, the warrant must be honored.

An issue presented in *United States v. Microsoft Corporation* led to the CLOUD Act’s provision on foreign-stored data.⁹⁰ In 2013, the federal government investigated a drug-trafficking operation and sought a warrant under the SCA to require Microsoft to produce all emails and information associated with an account hosted by Microsoft.⁹¹ The emails the government sought were stored on a server owned by Microsoft and located

⁸⁴ The authors are grateful to Zero Abuse Project’s legal extern Kiley Eichelberg for her research contributions.

⁸⁵ THE PURPOSE AND IMPACT OF THE CLOUD ACT, *supra* note 36.

⁸⁶ *The CLOUD Act*, EPIC ELEC. PRIV. INFO. CTR. (Oct. 29, 2019), <https://epic.org/privacy/cloud-act/> [<https://perma.cc/LUL6-V4E6>].

⁸⁷ *Id.*

⁸⁸ 18 U.S.C. § 2713 (2018).

⁸⁹ 18 U.S.C. § 2703(h)(1)(B) (2018) defines “United States person” by cross-referencing to 18 U.S.C. § 2523(a)(2) (2018) (“[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.”).

⁹⁰ *Microsoft Corp. v. United States*, 829 F.3d 197 (2d Cir. 2016), *vacated and remanded by United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018).

⁹¹ *Microsoft Corp.*, 138 S. Ct. at 1187.

in Dublin, Ireland.⁹² Microsoft challenged the search warrant's validity as applied to the emails, arguing that a United States magistrate does not have the jurisdiction to issue a warrant for digital information stored abroad.⁹³ A United States magistrate reviewed the challenge and held that a warrant under the SCA functions as a warrant and a subpoena—the latter of which is not restricted by territorial jurisdictional boundaries—and required Microsoft to turn over the emails.⁹⁴ A district judge upheld the magistrate's ruling.⁹⁵

Microsoft appealed to the Second Circuit. The United Kingdom Government filed an amicus brief, stating that if the United States government wished to obtain data located in Ireland, then the United States should use the MLAT between the United States and Ireland.⁹⁶ The Second Circuit overturned the district court's ruling, invalidating the warrant.⁹⁷ The court held the SCA cannot apply extraterritorially without explicit Congressional intent and found no such intent by Congress.⁹⁸ The Second Circuit denied the government's petition for a rehearing en banc.⁹⁹

The United States government filed a petition for certiorari in the United States Supreme Court in June 2017, which the Court granted in October 2017.¹⁰⁰ After the Court heard oral arguments, Congress introduced the CLOUD Act, which was signed into law on March 23, 2018.¹⁰¹ The CLOUD Act resolved the issues presented in *United States v. Microsoft Corp.*, and the Supreme Court declared the case moot.

B. *Bilateral Agreements*

The CLOUD Act addresses foreign governments' ability to access data stored in the United States in the course of criminal investigations.¹⁰² It does this by providing the authority to create bilateral agreements between the United States and other countries.¹⁰³ Presently, the United States has only entered into a bilateral agreement with the United Kingdom, though Australia has now paved the way through its domestic law to allow the

⁹² *Id.*

⁹³ *Id.*

⁹⁴ *Id.*

⁹⁵ *Id.*

⁹⁶ Brief of the Government of the United Kingdom of Great Britain and Northern Ireland as Amicus Curiae in Support of Neither Party, *United States v. Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016) (No. 17-2), 2017 WL 6398769.

⁹⁷ *Microsoft Corp.*, 829 F.3d at 201-02.

⁹⁸ *Id.* at 211.

⁹⁹ *Microsoft Corp. v. United States*, 855 F.3d 53 (2d Cir. 2017).

¹⁰⁰ *United States v. Microsoft Corp.*, 138 S. Ct. 356 (Oct. 16, 2017) (mem.).

¹⁰¹ *United States v. Microsoft Corp.*, 138 S. Ct. 1186, 1187 (2018).

¹⁰² *The CLOUD Act*, *supra* note 88.

¹⁰³ *Id.*

possibility of a future bilateral agreement with the United States.¹⁰⁴ Any nation wishing to enter into a bilateral agreement with the United States must be determined by the attorney general and secretary of state to meet the United States' high standards of due process and commitment to the rule of law.¹⁰⁵ Nations with adverse governmental philosophies will not be permitted to enter into a bilateral agreement with the United States.¹⁰⁶

Honoring warrants issued pursuant to the SCA and the CLOUD Act allows for a streamlined process, whereby the government may bypass

¹⁰⁴ Anne-Marie Allgrove, Adrian J. Lawrence, Toby Patten & Anne L. Petterd, *Australia - Bill Paves the Way for Australia-US Bilateral CLOUD Act Agreement and a New Cross-Border Data Access Regime*, LEXOLOGY (June 3, 2020), <https://www.lexology.com/library/detail.aspx?g=2cf0f5f7-4a6b-4523-b04c-4674296f9f74> [<https://perma.cc/T2PB-6XUC>].

¹⁰⁵ 18 U.S.C. § 2523(b)(4) (2018).

¹⁰⁶ *Id.* § 2523(b)(1). The U.S. attorney general with the concurrence of the secretary of state must provide a written certification to Congress averring, among other considerations, 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.

Id.

the cumbersome MLAT procedures.¹⁰⁷ The use of MLATs aims to protect human rights by requiring foreign governments to work with the Department of Justice to obtain warrants from United States judges before they can access that data for investigations.¹⁰⁸ Before the CLOUD Act, foreign governments needed a MLAT ratified by the United States Senate, approval from the Department of Justice, and authorization by a judge.¹⁰⁹ Now, foreign governments who have entered into a bilateral agreement with the United States may bypass this time-intensive process.

The CLOUD Act has received its fair share of criticism, mostly from those concerned about the international human rights implications of such unfettered access to data.¹¹⁰ However, because the CLOUD Act is still in its infancy, since the first bilateral agreement was entered rather recently (October 3, 2019),¹¹¹ we have yet to see if these concerns touted by privacy advocates have merit in the reality of the CLOUD Act's operations.

IV. UNITED STATES—UNITED KINGDOM BILATERAL AGREEMENT

The United States and the United Kingdom have come to a bilateral data-sharing agreement, as authorized by the CLOUD Act, which became effective July 8, 2020.¹¹² The agreement's purpose is to combat

¹⁰⁷ Taylor Hatmaker, *As the CLOUD Act Sneaks into the Omnibus, Big Tech Butts Heads with Privacy Advocates*, TECHCRUNCH (Mar. 22, 2018, 7:06 PM), <https://techcrunch.com/2018/03/22/cloud-act-omnibus-bill-house/> [<https://perma.cc/HC5Q-LZA5>].

¹⁰⁸ *Id.*

¹⁰⁹ *Id.*

¹¹⁰ In October 2019, twenty NGOs objected to the CLOUD Act, claiming it fails to protect privacy and due process rights of citizens. *The CLOUD Act*, *supra* note 88. See *Re: U.S.-U.K. CLOUD Act Agreement*, ELEC. PRIV. INFO. CTR. (Oct. 29, 2019), <https://epic.org/privacy/intl/USUK-CLOUD-Act-Letter-20191028.pdf> [<https://perma.cc/J49K-X6EJ>] for a list of the objections made by the organizations.

¹¹¹ *Agreement Between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime*, U.S. DEP'T OF JUST., <https://www.justice.gov/dag/cloud-act-agreement> [<https://perma.cc/A6SX-64D6>] [hereinafter *Agreement Between U.S. & U.K.*].

¹¹² *Supplementary Letter Conveyed to U.S. Congress in Support of U.S.-U.K. CLOUD Act Agreement*, U.S. DEP'T OF JUST. (Jan. 16, 2020), <https://www.justice.gov/dag/page/file/1236281/download> [<https://perma.cc/99FU-ABHL>]. The agreement enters into force 180 days after the attorney general provides notice to the Committee on the Judiciary and the Committee on Foreign Affairs of the House of Representatives, as well as the Committee on the Judiciary and the Committee on Foreign Relations of the Senate. *Id.* The attorney general transmitted notice to all required committees on December 4, 2019, but a clerical error rendered notice to the Committees of the House of Representatives ineffective. *Id.* The error was rectified on January 10, 2020 making the agreement effective on July 8, 2020. *Id.*

“serious crime, including terrorism.”¹¹³ The agreement serves as a mutual acknowledgment that the legal search and seizure frameworks of both the United States and the United Kingdom provide appropriate and substantial safeguards that protect the civil liberties of each country’s citizenry.¹¹⁴ Such mutual respect provides the rationale for using each country’s own domestic law for obtaining data that is stored by a covered provider¹¹⁵ subject to the exclusive jurisdiction of the other country.¹¹⁶

A. *Maintenance of Domestic Law*

As the data sharing agreement is predicated on mutual respect for the domestic law of the United States and the United Kingdom, each country is required to maintain its domestic law to meet the requirements of the data-sharing agreement.¹¹⁷ Each country is to ensure that its domestic law does not prevent providers from complying with the agreement.¹¹⁸ As a result, the data-sharing agreement restricts the United States’ ability to pass legislation that would effectively restrict law enforcement access to data stored by covered providers.¹¹⁹

Orders issued pursuant to the agreement are governed by the domestic law of the issuing country.¹²⁰ Effectively, this means that United States law enforcement can obtain data under this agreement from a United Kingdom covered provider through the United States’ legal process without interference from United Kingdom law, such as the General Data Protection Regulation (GDPR).¹²¹ This does not affect the provider’s right to raise applicable legal objections.¹²²

¹¹³ *Agreement Between U.S. & U.K.*, *supra* note 113, art. 2.1.

¹¹⁴ *Id.* art. 3.3.

¹¹⁵ *Id.* art. 1.7. “Covered Provider means any private entity to the extent that it: (i) provides to the public the ability to communicate, or to process or store computer data, by means of a Computer System or a telecommunications system; or (ii) processes or stores Covered Data on behalf of an entity defined in subsection (i).” *Id.*

¹¹⁶ *Id.* art. 3.3.

¹¹⁷ *Id.* art. 3.1.

¹¹⁸ *Id.*

¹¹⁹ *Id.*

¹²⁰ *Id.* art. 3.2.

¹²¹ *Id.* The United Kingdom’s exit from the European Union, commonly known as Brexit, will likely have an impact on the U.S.-U.K. agreement because the United Kingdom will no longer require adherence to the GDPR, as this was a law under the European Union. *Information Rights at the End of the Transition Period Frequently Asked Questions*, INFO. COMM’R’S OFF., https://ico.org.uk/media/for-organisations/documents/brexit/2617110/information-rights-and-brexit-faqs-v2_3.pdf [<https://perma.cc/9WEM-BL38>]. The United Kingdom plans to create its own GDPR, which will directly incorporate the European Union’s GDPR. *Id.*

¹²² *Agreement Between U.S. & U.K.*, *supra* note 113, art. 3.2.

The United Kingdom allows the United States to compel the production of data through the United States' domestic law because the United Kingdom recognizes the United States' privacy and civil rights safeguards.¹²³ Should the United States loosen those safeguards, it is required to notify the United Kingdom.¹²⁴

The agreement does not create a private right of action to obtain, suppress, or exclude evidence or to impede execution of legal process.¹²⁵ However, domestic law may provide a remedy; invoking the data sharing agreement is not blanket immunization from civil penalties, nor is it an escape from the grasp of the Fourth Amendment.¹²⁶

B. Proper Targeting

Orders issued under the agreement must have a proper target with respect to both the crime and the person under investigation.¹²⁷ An order targeting a proper crime has the purpose of preventing, investigating, detecting, or prosecuting a covered offense.¹²⁸ A covered offense is a "Serious Crime, including terrorist activity."¹²⁹ A serious crime must carry a maximum sentence of at least three years imprisonment.¹³⁰

Orders issued under this agreement cannot intentionally target a receiving-party person.¹³¹ A receiving-party person is one who, "[w]here the United Kingdom is the Receiving Party," is a:

Governmental entity or authority of the state; . . . an unincorporated association, a substantial number of members of which are located in [the territories of the United Kingdom]; . . . a corporation located or registered in [the territory of the United Kingdom]; or any other person located in [the territory of the United Kingdom].¹³²

In other words, an order under the data-sharing agreement issued by United States law enforcement cannot target the account of a person or entity located in the United Kingdom.

Additionally, orders under this agreement may not be used to target a valid person under the agreement "if the purpose is to obtain information

¹²³ *Id.* art. 3.3.

¹²⁴ *Id.*

¹²⁵ *Id.* art. 3.4.

¹²⁶ *Id.* art. 3.2.

¹²⁷ *Id.* art. 4.1, 4.3-4.

¹²⁸ *Id.* art. 4.1.

¹²⁹ *Id.* art. 1.5.

¹³⁰ *Id.* art. 1.14.

¹³¹ *Id.* art. 4.3.

¹³² *Id.* art. 1.12.

concerning a Receiving-Party Person.”¹³³ All orders must target specific accounts and must include a specific identifier for the account.¹³⁴ Law enforcement officers cannot use the agreement to infringe upon freedom of speech, nor may it be used to “disadvantage persons based on their race, sex, sexual orientation, religion, ethnic origin, or political opinions.”¹³⁵

C. *Issuance and Transmission of Orders*

United States law enforcement can seek an order compelling the disclosure of information or for the preservation of data¹³⁶ under the agreement using the domestic laws of the United States.¹³⁷ However, orders under the agreement must be based on minimum requirements “for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation.”¹³⁸ As orders must be in compliance with domestic law, when domestic law imposes a stricter standard, such a standard must be met.¹³⁹

For United States law enforcement officers, this means that the Electronic Communications Privacy Act will likely dictate the process to obtain data stored by UK-based service providers.¹⁴⁰ Additionally, an order for the production of data under this agreement is subject to review and/or oversight under domestic law of the United States.¹⁴¹ In this respect, independent oversight occurs in the issuance of an order under this agreement, and such oversight is dictated by the domestic legal authority under which the order is authorized.¹⁴²

As with domestic orders, when an order seeks interception of wire or electronic communications, the order must be for a fixed and limited duration, cannot last longer than is reasonably necessary, and the information sought must not be reasonably obtainable through less intrusive means.¹⁴³ Orders under this agreement cannot be issued with the purpose

¹³³ *Id.* art. 4.4.

¹³⁴ *Id.* art. 4.5.

¹³⁵ *Id.* art. 4.2.

¹³⁶ *See generally id.* art. 10. The same rules that apply to compelling disclosure of information stored by a covered provider also apply to preservation orders. *See id.*

¹³⁷ *Id.* art. 5.1.

¹³⁸ *Id.*

¹³⁹ *Id.*

¹⁴⁰ Some states like California may have strict laws similar to the ECPA that limit the type, manner, or method of obtaining data covered by the ECPA. Be sure to consult both state and federal law in your jurisdiction prior to your investigation.

¹⁴¹ *Agreement Between U.S. & U.K.*, *supra* note 113, art. 5.2.

¹⁴² *Id.*

¹⁴³ *Id.* art. 5.3.

of providing the information obtained to the United Kingdom or a third party.¹⁴⁴

Orders are to be directly served on the covered provider by the designated authority of the issuing party.¹⁴⁵ The designated authority for the United States is the attorney general.¹⁴⁶ The attorney general may delegate duties to additional authorities and set rules and conditions for any additional authorities.¹⁴⁷ All orders must be reviewed by the attorney general, or his designee, prior to serving them upon providers.¹⁴⁸ The attorney general must certify that the order complies with the domestic laws of the United States and that the order fully complies with the agreement.¹⁴⁹ The provider must be notified that the order is issued pursuant to the agreement and granted “a point of contact . . . who can provide information on legal or practical issues relating to the Order.”¹⁵⁰ If the target of the order is not a citizen of the United States and is located outside the territory of the United States, the attorney general, or his designee, is to notify the relevant authorities in the third country where the target is located, unless the “notification would be detrimental to operational or national security, impede . . . the investigation, or imperil human rights.”¹⁵¹

The provider can object to an order issued under the agreement.¹⁵² The provider must raise any objections in a reasonable time to the attorney general.¹⁵³ The attorney general may then respond to the objections.¹⁵⁴ If the objections are not resolved, the provider may raise the objections with the United Kingdom’s designated authority.¹⁵⁵ The attorney general and the United Kingdom’s designated authority may confer to resolve the objections.¹⁵⁶ If the objections cannot be resolved between the authorities, then the United Kingdom’s designated authority must notify the attorney general that the agreement shall not apply to the order.¹⁵⁷ The bilateral

¹⁴⁴ *Id.* art. 5.4.

¹⁴⁵ *Id.* art. 5.5.

¹⁴⁶ *Id.* art. 1.8.

¹⁴⁷ *Id.* art. 5.5.

¹⁴⁸ *Id.* art. 5.6.

¹⁴⁹ *Id.* art. 5.7. The certification must be in writing and included with the order when transmitted to the covered provider. *Id.*

¹⁵⁰ *Id.* art. 5.8–9.

¹⁵¹ *Id.* art. 5.10.

¹⁵² *Id.* art. 5.11. Objections must be specific and based on a reasonable belief that the agreement has not been properly invoked. *Id.*

¹⁵³ *Id.* The agreement does not state what constitutes a reasonable time. *See id.*

¹⁵⁴ *Id.*

¹⁵⁵ *Id.*

¹⁵⁶ *Id.*

¹⁵⁷ *Id.* art. 5.12.

agreement does not explicitly provide for judicial review of a provider's objection.¹⁵⁸

D. Production of Information

When an order is properly served on a covered provider, and all objections have been settled, the covered provider is to produce the requested information directly to the attorney general.¹⁵⁹ The attorney general and the provider may make arrangements for the secure transmission of the order and the information requested in the order.¹⁶⁰ To aid in the admissibility of evidence obtained through the agreement, law enforcement officers may require the provider to complete forms attesting to the authenticity of the records produced or to the absence or non-existence of such records.¹⁶¹

E. Minimization Procedures

The agreement requires the United States to develop a procedure for ensuring that the targeted account belongs to someone covered by the agreement.¹⁶² The procedures must be employed in good faith and with reasonable effort to avoid targeting receiving-party persons.¹⁶³

F. Limitations on Use and Transfer

United States law enforcement is to handle data received through the agreement in accordance with the domestic laws of the United States.¹⁶⁴ For example, if the information collected under the agreement would be protected by privacy laws or subject to a Freedom of Information Act request if collected under domestic law, the information is still covered by those privacy and freedom of information laws.¹⁶⁵

United States law enforcement cannot transfer data obtained under the agreement to a third country or international organization without the United Kingdom's consent, unless the data has already been made public.¹⁶⁶ Additionally, the agreement expressly prohibits requirements that the

¹⁵⁸ See generally *id.* art.1-17.

¹⁵⁹ *Id.* art. 6.1.

¹⁶⁰ *Id.* art. 6.2.

¹⁶¹ *Id.* art. 6.4.

¹⁶² *Id.* art. 7.1.

¹⁶³ *Id.*

¹⁶⁴ *Id.* art. 8.1.

¹⁶⁵ *Id.*

¹⁶⁶ *Id.* art. 8.2.

United States share information obtained under the agreement with the United Kingdom or with any third-party government and vice versa.¹⁶⁷

Moreover, both the United States and the United Kingdom have specialized national interests implicated by the agreement. For United States law enforcement seeking data from a United Kingdom service provider, the United Kingdom has a particularly strong interest in the death penalty.¹⁶⁸ When United States law enforcement seeks data from the United Kingdom, it must ask for and receive permission from the United Kingdom in order to use evidence obtained under this agreement in a death penalty case.¹⁶⁹ The United Kingdom may deny permission, grant permission, or grant permission subject to conditions of use.¹⁷⁰ The same is true when the United Kingdom seeks information from the United States where freedom of speech is implicated.¹⁷¹ Additional limits may be set as mutually agreed upon by both parties.¹⁷²

G. Compatibility and Non-Exclusivity

The agreement does not affect any other legal authorities or mechanisms for preserving or obtaining electronic data.¹⁷³ The agreement does not affect legal instruments issued under the domestic law of either party, requests for mutual legal assistance, or emergency disclosures.¹⁷⁴

H. Expiry and Termination of the Agreement

The agreement is in effect until July 8, 2025.¹⁷⁵ The United States and the United Kingdom may agree to extend the agreement by agreeing, in writing, through diplomatic channels.¹⁷⁶ By the same token, the agreement may be terminated by either party by sending written notice through diplomatic channels.¹⁷⁷ Termination will be effective one month after the date of such notice.¹⁷⁸ Should the agreement expire or be terminated, any data produced under the agreement may continue to be used but must

¹⁶⁷ *Id.* art. 8.3.

¹⁶⁸ *Id.* art. 8.4(a).

¹⁶⁹ *Id.* art. 8.4.

¹⁷⁰ *Id.*

¹⁷¹ *Id.* art. 8.4(b).

¹⁷² *Id.* art. 8.5.

¹⁷³ *Id.* art. 11.1.

¹⁷⁴ *Id.*

¹⁷⁵ *Id.* art. 17.1. The agreement has a term of five years from the date the agreement enters into force. *Id.*

¹⁷⁶ *Id.*

¹⁷⁷ *Id.* art. 17.2.

¹⁷⁸ *Id.*

continue to be subject to the conditions and safeguards of the agreement.¹⁷⁹
Each party bears its own costs arising from the operation of the agreement.¹⁸⁰

V. HOW PROSECUTORS AND LAW ENFORCEMENT CAN OBTAIN REMOTELY STORED DATA¹⁸¹

A. *Search Warrants and Digital Evidence*

The Fourth Amendment to the United States Constitution guarantees the “right of the people to be secure in their persons, houses, papers, and effects . . . and no warrants shall issue, but upon probable cause . . . particularly describing the place to be searched, and the persons or things to be seized.”¹⁸² Generally speaking, the probable cause element of the Fourth Amendment is met when the affiant describes why, in their training and experience, digital evidence will be found in the place to be searched and is relevant to the crime under investigation.¹⁸³ While the standard is not proof beyond a reasonable doubt, the items sought must have a nexus to the place being searched, with a “fair probability,” based on common sense, that said items will be found in the location.¹⁸⁴

The items to be searched equally must be sufficiently described to avoid the government from unfettered searches of a location not otherwise relevant to the crime under investigation.¹⁸⁵ Because digital evidence can physically be contained on thumb drives the size of a thumbnail and obfuscated by digital “booby traps,” the warrant may necessitate an extensive search of the device limited by the crime.¹⁸⁶

There equally must be a finding that the evidence sought will be at the location when law enforcement conducts its search. Unlike guns and drugs, which are easily disposed of by a criminal, digital evidence is “not the type of evidence that rapidly dissipates or degrades”¹⁸⁷ when located on a *physical* device:

When you delete a file, it goes into a “trash” folder, and when you direct the computer to “empty” the trash folder

¹⁷⁹ *Id.* art. 17.3.

¹⁸⁰ *Id.* art. 13.

¹⁸¹ Case studies included in this section and throughout this publication are works of fiction. Names, characters, entities, places, and incidents either are products of the author’s imagination or are used fictitiously. Any resemblance to actual events or locales or persons, living or dead, is entirely coincidental.

¹⁸² U.S. CONST. amend. IV.

¹⁸³ *United States v. Bowen*, 689 F. Supp. 2d 675, 679–80 (S.D.N.Y. 2010).

¹⁸⁴ *Illinois v. Gates*, 462 U.S. 213, 214 (1983).

¹⁸⁵ *United States v. Riley*, 906 F.2d 841, 845 (2d Cir. 1990).

¹⁸⁶ *Id.* at 845 (“[F]ew people keep documents of their criminal transactions in a folder marked ‘drug records.’”).

¹⁸⁷ *United States v. Vosburgh*, 602 F.3d 512, 529 (3d Cir. 2010).

the contents of the folder, including the deleted file, disappear. But the file hasn't left the computer. The trash folder is a waste-paper basket; it has no drainage pipe to the outside. The file *seems* to have vanished only because the computer has removed it from the user interface and so the user can't "see" it any more.¹⁸⁸

As Judge Posner observed in *Seiver*, it is possible that the file could be overwritten if the hard drive of the computer is exhausted.¹⁸⁹ To accomplish this task, however, the user would have to exhaust the significant size of modern hard drives. Even if overwritten, common sense dictates that the basic user of digital devices saves their data on a cloud or external hard drive, thus evidence still likely exists at the location where law enforcement seeks it. Consequently, though there are multiple possibilities that data could be encrypted, overwritten, or wiped, "rarely will [these possibilities] be so probable as to destroy probable cause."¹⁹⁰ Judge Posner further observed that:

No doubt after a *very* long time, the likelihood that the defendant still has the computer, and if he does that the file hasn't been overwritten, or if he's sold it that the current owner can be identified, drops to a level at which probable cause to search the suspect's home for the computer can no longer be established. But seven months is too short a period to reduce the probability that a computer search will be fruitful to a level at which probable cause has evaporated. . . . The most important thing to keep in mind for future cases is the need to ground inquiries into "staleness" and "collectors" in a realistic understanding of modern computer technology and the usual behavior of its users.¹⁹¹

Judge Posner's rationale has been met with significant approval by other courts.¹⁹² This reasoning, however, should not suggest that probable cause to search a location or device will never go stale but that law enforcement should sufficiently articulate the fact that remnants of data are not easily destroyed over time.

¹⁸⁸ United States v. *Seiver*, 692 F.3d 774, 776 (7th Cir. 2012).

¹⁸⁹ *Id.* at 777.

¹⁹⁰ *Id.*

¹⁹¹ *Id.* at 777-78.

¹⁹² See United States v. *Valley*, 755 F.3d 581, 586-87 (2014) ("But as *Seiver* makes clear . . . investigators looking for digital evidence can assume it remains on the hard drive because modern computers by default retain the data."); United States v. *Carroll*, 750 F.3d 700, 707 (2014) (applying Judge Posner's analysis in rejecting a staleness challenge to the search of Carroll's digital devices for child sexual abuse material, despite a delay of sixty months).

In reviewing affidavits, prosecutors must ensure that warrant applications adequately describe the location to be searched, what evidence may be found at the location and where it may be found, and why it would be found there despite the passage of time.¹⁹³ These descriptions must be based on a realistic understanding of technology, not mere rumor or happenstance.¹⁹⁴ Prosecutors must be mindful that data may not be stored on a device but rather held by a cloud service provider. Unlike the physical digital device, data can be easily deleted from cloud storage. This information, if preserved by the mechanisms described in the Electronic Communications Privacy Act, allows law enforcement to ensure key data is not deleted.

B. Obtaining Domestically Stored Data

Currently, the most frequent remote data storage scenarios facing United States law enforcement involve the need to acquire data stored on a server somewhere in the United States. Since data storage continues to proliferate in frequency and sophistication, this may not always be the case.¹⁹⁵ Regardless of the server's location, however, legal process should be directed to the internet service provider, not the individual server's location.

This is logical for several reasons. First, the prospect of law enforcement serving legal process on the location of a server is unrealistic since law enforcement will lack knowledge of the server's location, and the provider may move the data at any time. Second, data can be stored anywhere; servers often exist across national boundaries and around the world.¹⁹⁶ Third, data is often not stored in any one location. The common practice of sharding involves splitting up data and distributing it among multiple locations.¹⁹⁷

International law recognizes and addresses data location concerns. The Convention on Cyber Crime, or Budapest Convention, mandates that all signatory countries maintain the ability to use legal processes to compel companies to produce electronic data they control, even when the company

¹⁹³ *Id.*

¹⁹⁴ *Id.*

¹⁹⁵ *See generally infra* Section V.E.

¹⁹⁶ *See infra* Section V.E.

¹⁹⁷ Jeeyoung Kim, *How Sharding Works*, MEDIUM (Dec. 5, 2014), <https://medium.com/@jeeyoungk/how-sharding-works-b4dec46b3f6> [<https://perma.cc/T469-RRTR>]. For an important analysis of forensic science concerns in cloud computing ecosystems, see MARTIN HERMAN ET AL., NAT'L INST. OF STANDARDS & TECH., NIST CLOUD COMPUTING FORENSIC SCIENCE CHALLENGES (2020), <https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8006.pdf> [<https://perma.cc/JN3B-MDYK>].

stores the data in another country.¹⁹⁸ The Department of Justice has noted that the CLOUD Act “makes explicit in U.S. law the long-established U.S. and international principle that a company subject to a country’s jurisdiction can be required to produce data the company controls, regardless of where it is stored at any point in time.”¹⁹⁹

Given the irrelevance of the data’s location, law enforcement must identify the relevant internet-service provider(s) with access to the desired evidence and immediately send a letter of preservation. The SCA mandates that upon a governmental entity’s request, a provider “shall take all necessary steps to preserve records and other evidence in its possession,” pending further legal process.²⁰⁰ This initial request is valid for ninety days and may be extended for an additional ninety days.²⁰¹ Preserving data is a critical tool to prevent destruction or loss of evidence while obtaining additional legal authority. Investigators or prosecutors failing to take this step unnecessarily compromise critical evidence in criminal cases, potentially by a suspect’s overt acts, such as deleting content or accounts or using remote wiping programs or signals, or automated actions of the service provider, such as routine deletion processes.²⁰²

After sending a letter of preservation, the appropriate method of legal process must be selected. This analysis arguably differs depending on whether the prosecutor’s approach is based on a strict textual analysis of the SCA or a proactive recognition of the trajectory of Fourth Amendment jurisprudence. The latter is required to avoid suppression of evidence²⁰³ and problematic case law, given the trend of privacy-oriented judicial opinions and greater scrutiny of law enforcement’s reliance on traditional Fourth Amendment doctrines.²⁰⁴

For a strict textual analysis, guidance for legal process is found in the SCA, 18 U.S.C. § 2701, *et seq.* Multiple methods of legal process are set forth in 18 U.S.C. § 2703 depending on the circumstances. More specifically, if the information sought is the contents of a wire or electronic

¹⁹⁸ Council of Europe Convention on Cybercrime art. 21, *opened for signature* Nov. 23, 2001, C.E.T.S. No. 185 (entered into force Jan. 7, 2004). For an official list of participating countries, see *Chart of Signatures and Ratifications of Treaty 185: Convention on Cyber Crime*, COUNCIL OF EUROPE, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=cmPs1otx [<https://perma.cc/83D4-EQA8>]; see also THE PURPOSE AND IMPACT OF THE CLOUD ACT, *supra* note 36.

¹⁹⁹ THE PURPOSE AND IMPACT OF THE CLOUD ACT, *supra* note 36.

²⁰⁰ 18 U.S.C. § 2703(f)(1) (2018).

²⁰¹ *Id.* § 2703(f)(2).

²⁰² “A remote wipe generally refers to the deleting of data on a device During a remote wipe, the deletion is triggered from a remote system endpoint.” *Remote Wipe*, TECHOPEDIA, <https://www.techopedia.com/definition/10352/remote-wipe> [<https://perma.cc/3WCJ-X7ZB>].

²⁰³ See *Carpenter v. United States*, 138 S. Ct. 2206, 2209–10 (2018).

²⁰⁴ See *supra* Section II.C.

communication and has been in electronic storage for 180 days or less, § 2703(a) requires a search warrant pursuant to the Federal Rules of Criminal Procedure or in “[s]tate court, issued using [s]tate warrant procedures”²⁰⁵ These search warrants must be issued “by a court of competent jurisdiction,” whether state or federal.²⁰⁶ The SCA defines this broadly as “a court of general criminal jurisdiction of a [s]tate authorized by the law of that [s]tate to issue search warrants”²⁰⁷

If the information is the contents of a wire or electronic communication, and it has resided in electronic storage for more than 180 days, § 2703(b) applies and permits a couple of options for legal process. The first of these is a search warrant using the same procedures as those listed in § 2703(a). The second option is by obtaining an administrative subpoena²⁰⁸ or a court order under § 2703(d). Any “court of competent jurisdiction”²⁰⁹ may issue 2703(d) orders. The thresholds for obtaining subpoenas and 2703(d) orders are lower than probable cause; to obtain a 2703(d) order, law enforcement must offer “specific and articulable facts showing that there are reasonable grounds to believe” that the information sought is “relevant and material to an ongoing criminal investigation.”²¹⁰ This lower standard has great significance, as demonstrated by the outcome and analysis of the Supreme Court in *Carpenter v. United States*.²¹¹

Notably, the SCA does not require notice to the account holder when law enforcement uses legal process to access account content. However, a specific provision of the SCA permits delaying the legal process notification to the account holder if requested by law enforcement and approved by a court issuing an order to delay the notification.²¹² In light of privacy-oriented judicial trajectories and the risk of evidence loss, law enforcement officers should err on the side of caution and always include a delay in notification application and court order authorizing delayed notice to an account holder. A court may delay the notification for a period of ninety days.²¹³ In ongoing investigations, law enforcement may request that a court extend the notification delay in increments of additional ninety days upon application and court order.²¹⁴

²⁰⁵ 18 U.S.C. § 2703(a) (2018).

²⁰⁶ *Id.*

²⁰⁷ *Id.* § 2711(3)(B).

²⁰⁸ Administrative subpoenas must be “authorized by a [f]ederal or [s]tate statute or a [f]ederal or [s]tate grand jury or trial subpoena.” *Id.* § 2703(b)(1)(B)(i).

²⁰⁹ *Id.* § 2703(d).

²¹⁰ *Id.*

²¹¹ *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

²¹² 18 U.S.C. § 2705 (2018).

²¹³ *Id.*

²¹⁴ *Id.*

If law enforcement is seeking to obtain non-content records of electronic communications, 18 U.S.C. § 2703(c) authorizes four methods: “consent of the subscriber or customer,” subpoena, 2703(d) order, or search warrant.²¹⁵ Non-content records may include the subscriber’s name; address, telephonic session times and durations; length of service including start dates and service types; telephone number and other subscriber identifiers; and the means and payment sources for the account.²¹⁶ Obtaining this information by subpoena often provides critical leads and corroboration for law enforcement. Examples include establishing a suspect’s identity in the early stages of investigation and obtaining information to satisfy the probable cause threshold necessary for search warrants requesting authorization to examine communication contents. Google’s subpoena returns provide an excellent example of the information law enforcement may uncover using a subpoena. Generally, the Google subpoena response may include names, phone numbers, and email addresses associated with the Google account; time and date of last logins; and specific IP addresses used, among other information. Equally enlightening, the return also lists any Google services used by that subscriber, such as Google Calendar, Google Photos, and location history. Individually or collectively, the subscribers’ Google services data could corroborate allegations or provide specific Google products to target with a search warrant.²¹⁷

Even though multiple methods of obtaining content exist under § 2703(b), a search warrant is the most appropriate option. From a practical standpoint, in many cases, investigators possessing specific and articulable facts sufficient to meet § 2703(d)’s threshold are most likely able to meet the probable cause threshold to secure a search warrant. For law enforcement confronted with the choice of using either a § 2703(d) order or a search warrant, a search warrant is the wiser option. Data secured through a search warrant supported by probable cause flips the burden to a defendant to demonstrate a basis for declaring the search warrant invalid and suppressing the evidence.

The trajectory of Fourth Amendment jurisprudence illustrates the wisdom of the maxim “When in doubt, get a search warrant,”²¹⁸ evidencing greater sensitivity to privacy concerns, even in the context of long-established

²¹⁵ *Id.* § 2703(c)(1).

²¹⁶ *Id.* § 2703(c)(2).

²¹⁷ Information represented by Google in August 2020. Google made these representations during a workshop presented for the 2020 Crimes Against Children Conference. The workshop itself is no longer accessible at cacconference.org, but the workshop was attended by the author(s), and the information is consistent with the authors’ prosecutorial practice. This is a critical practice pointer that unfortunately most prosecutors (and other attorneys) are unaware of.

²¹⁸ *See supra* Part II.

and rarely-questioned doctrines. In several prior cases, the United States Supreme Court “held repeatedly” information conveyed to a third party, even if only for a “limited purpose” or in “confidence,” enjoyed no Fourth Amendment protection.²¹⁹ The prior decisions ruled a person lacked a reasonable “expectation of privacy in information voluntarily turned over to third parties.”²²⁰

As integration of technology in daily life became ubiquitous, however, courts began to develop and apply heightened Fourth Amendment protections. In *Riley v. California*, the Supreme Court prohibited warrantless cell phone searches, “even when a cell phone is seized incident to arrest.”²²¹ The Court reasoned that cell phones “are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans ‘the privacies of life.’”²²²

The *Carpenter* Court applied a similar privacy-oriented analysis to impose a new search warrant supported by probable cause threshold to obtain cell site location information (CSLI).²²³ In that case, law enforcement used a § 2703(d) order to obtain CSLI data.²²⁴ The Court specifically rejected the third-party doctrine’s application to CSLI data, holding that the context of CSLI being “gathered by a third party does not make it any less deserving of Fourth Amendment protection.”²²⁵ The Court concluded that the use of the § 2703(d) order’s lower threshold of “specific and articulable facts” failed to satisfy an individual’s reasonable expectation of privacy in the data.²²⁶ Contradictory to the legal process provisions within the SCA, especially § 2703(b), the decision eviscerates a court order’s effectiveness to obtain transactional data.

The Sixth Circuit’s decision in *United States v. Warshak*²²⁷ exemplifies the peril of relying on the SCA’s legal process provisions to obtain communications content. In *Warshak*, law enforcement sent a letter of preservation pursuant to 18 U.S.C. § 2703(f) and followed up with legal process—specifically, an administrative subpoena as authorized by the text of § 2703(b) for disclosure of emails over 180 days old.²²⁸ Contrary to the SCA’s procedural mandates, the Sixth Circuit found that a reasonable expectation of privacy existed in the emails’ content obtained by law

²¹⁹ *United States v. Miller*, 425 U.S. 435, 443 (1976).

²²⁰ *Carpenter v. United States*, 138 S. Ct. 2206, 2209 (2018) (citing *Miller*, 425 U.S. at 435; *Smith v. Maryland*, 442 U.S. 735 (1979)).

²²¹ *Riley v. California*, 573 U.S. 373, 401 (2014).

²²² *Id.* at 403 (citation omitted).

²²³ *See Carpenter*, 138 S. Ct. at 2209–10.

²²⁴ *Id.* at 2212.

²²⁵ *Id.* at 2223.

²²⁶ *Id.* at 2209, 2212.

²²⁷ 631 F.3d 266 (6th Cir. 2010).

²²⁸ *Id.* at 283; *see* 18 U.S.C. § 2703(a) (2018).

enforcement and imposed a warrant requirement.²²⁹ The *Warshak* court ruled that the Fourth Amendment required law enforcement to procure a search warrant authorizing the examination of the emails' content.²³⁰ The court rejected the SCA's delineation in § 2703(b) of legal process categories; the length of email storage was irrelevant to the court's analysis.²³¹ The *Warshak* court determined law enforcement's failure to use a search warrant to access the email content violated the Fourth Amendment.²³² Additionally, the court found the relevant portion of the SCA was unconstitutional.²³³

When the remote computing service or electronic communications service refuses to honor the issued legal process, the prosecutor should zealously advocate for enforcing the subpoena, court order, or search warrant.²³⁴ As the chief law enforcement officer in the jurisdiction, a prosecutor has a duty to investigate the basis for the legal objection, engage in negotiations, and, where appropriate, secure the production of the requested records through a motion to compel or order to show cause.

Whether a case resides in federal or state court, the judiciary possesses the inherent authority to compel and sanction a party for noncompliance with a lawfully served subpoena, court order, or search warrant. The judiciary's elemental power emanates from constitutional, statutory, and court-developed rules—without which, a court would be powerless over the attorneys or litigants who appear before the bench. A subpoenaed party may seek relief from the judge when there is reason to question a document's validity or the authority to issue the subpoena. A party failing to request judicial review usurps judicial authority, potentially acting contemptuously. If this standard applies to subpoenas, then the same reasoning retains even greater import when an *ex parte* modification to a search warrant occurs.²³⁵

²²⁹ *Warshak*, 631 F.3d at 286.

²³⁰ *Id.* at 288.

²³¹ *Id.*

²³² *Id.*

²³³ *Id.*

²³⁴ For instance, an ISP/ESP has no right to stand in the shoes of their customer and assert a right of privacy in response to a validly issued warrant. *See In re 381 Search Warrants to Facebook, Inc.*, 78 N.E.3d 141, 143, 153 (N.Y. 2017). The ISP/ESP has a limited right to review in a subpoena/court order. *Id.* at 147-49.

²³⁵ Service provider remedies are often limited in the context of search warrants. *See id.* at 145-49 (finding that an order denying Facebook's motion to quash a search warrant was not appealable).

1. *Costs Associated with Obtaining the Data*

In exchange for producing the data, a remote computing service or electronic communications service may seek reimbursement for costs “*directly incurred* in searching for, assembling, reproducing, or otherwise providing such information.”²³⁶ The amount of such reimbursement shall be mutually agreed upon by the government and the remote computing service and/or electronic communications service.²³⁷ If the parties do not reach an agreement, the court, where the legal process originated or where the criminal action commences, shall decide the amount of reimbursement owed.²³⁸

Interestingly, 18 U.S.C. § 2706(c) exempts communications common carriers from seeking cost reimbursement from law enforcement for telephone toll records and telephone listings.²³⁹ When Congress enacted the Electronic Communications Privacy Act in 1986, Congress did not intend to compensate service providers for the costs of routine requests for subscriber and toll information.²⁴⁰

Since the SCA’s passage in 1986, technology advanced from the basic days of dial-up internet services Prodigy, CompuServe, and Juno to Google and Yahoo. Likewise, the legal process for subscriber information, internet protocol logs, and content increased.²⁴¹ With the growth of technology, remote computing service, and electronic communication service, providers have expanded legal compliance departments and leveraged technology to access data for the consumer’s benefit as well as accommodate the increase in legal process for subscriber information, internet protocol logs, and content.²⁴² This increase in legal process is likely attributable to the increased use of technology to commit a crime. Arguably, the statutory intent in exempting common communications carriers from seeking cost reimbursement from law enforcement for telephone toll records and telephone listings may now apply for a majority of legal

²³⁶ 18 U.S.C. § 2706(a) (2018) (emphasis added).

²³⁷ *Id.* § 2706(b).

²³⁸ *Id.*

²³⁹ *Id.* § 2706(c).

²⁴⁰ See *Mich. Bell Tel. Co. v. Drug Enf’t Admin.*, 693 F. Supp. 542, 544 (E.D. Mich. 1988).

²⁴¹ See, e.g., *Dropbox Legal Transparency Report*, DROPBOX, <https://www.dropbox.com/transparency/reports> [https://perma.cc/P58A-2ND9]; *Google Transparency Report: Requests for User Information*, GOOGLE, <https://transparencyreport.google.com/user-data/overview> [https://perma.cc/4HCW-7H55]; *Verizon Media Government Data Requests*, VERIZON MEDIA, <https://www.verizonmedia.com/transparency/reports/government-data-requests.html> [https://perma.cc/6EU7-Y2WB].

²⁴² See, e.g., *Dropbox Legal Transparency Report*, *supra* note 243; *Google Transparency Report: Requests for User Information*, *supra* note 243; *Verizon Media Government Data Requests*, *supra* note 243.

demands to remote computing service and electronic communication service providers.

The plain wording of 18 U.S.C. § 2706 equally suggests that a remote computing service or electronic communication service provider cannot withhold data pending payment.²⁴³ Indeed, 18 U.S.C. § 2706 states that “a governmental entity . . . shall pay . . . a fee for *reimbursement* for such costs . . . *directly incurred* in . . . providing such information.”²⁴⁴ The use of the past tense in the word *incurred*, coupled with the present tense usage of the word *reimbursement*,²⁴⁵ indicates that the records already have been produced for a duly served piece of legal process.

What is more, the plain wording refers to expenses *directly related* to the production.²⁴⁶ Providers should not be permitted to obtain financial benefits beyond the intent of 18 U.S.C. § 2706, and prosecutors or law enforcement receiving an inordinate bill from a service provider should avail themselves of the court of original jurisdiction to resolve the disputed amount.

The following hypothetical illustrates the process of obtaining remotely-stored data on servers within the United States.²⁴⁷ John, a forty-three-year-old man residing in Midgard (the newest state admitted to the United States), began texting with a fourteen-year-old female, Stacy, after ending his relationship with Stacy’s mom. John sent Stacy explicit chats, resulting in John asking Stacy to meet him for a sexual encounter. During the in-person meeting, John committed several sex acts against Stacy, all of which John recorded using his nPhone. In addition to John’s nPhone saving pictures and videos directly to the phone, John configured his nPhone to automatically save a duplicate of any photo or video created with the phone to John’s nCloud account. nCloud is a cloud-based storage service owned and operated by Nectarine. Nectarine is a company headquartered in California, and Nectarine servers (which host the nCloud data) are in Virginia. John, suspecting the police knew about his criminal acts with Stacy, performed a factory reset of his nPhone, destroying all data (including chats and photos) on his nPhone.

However, performing the factory reset did not remove the photos or chats from John’s nCloud account, and John did not delete the data from

²⁴³ See H. MARSHALL JARRETT, MICHAEL W. BAILIE, ED HAGEN & NATHAN JUDISH, *SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS* 127 (2009) (“Section 2703 offers five mechanisms that a “government entity” can use to compel a provider to disclose certain kinds of information.”).

²⁴⁴ 18 U.S.C. § 2706(a) (2018) (emphasis added).

²⁴⁵ “[T]he act of paying back money to someone who has spent it for you or lost it because of you, or the amount that is paid back.” *Reimbursement*, CAMBRIDGE DICTIONARY, <https://dictionary.cambridge.org/dictionary/english/reimbursement> [<https://perma.cc/HT5S-WRD9>].

²⁴⁶ 18 U.S.C. § 2706(a) (2018).

²⁴⁷ See *supra* Part I.

his nCloud account. Following Stacy's disclosure to her guidance counselor, the police learned of John's manipulation and sexual assault. Officer Kay Oss, of the Midgard State Police, responded to the guidance counselor's report and opened an investigation. Officer Oss wants to obtain the chats and photos from John's nCloud account. Officer Oss is uncertain what legal process to use since the servers are in Virginia and not Midgard.

2. *How Should the Midgard Prosecutors Advise Officer Oss?*

Officer Oss should immediately send a letter of preservation to Nectarine. If Officer Oss is unsure where and how to send the preservation letter, she could access an investigative resource such as search.org, specifically SEARCH's Internet Service Provider (ISP) List; ask her local prosecutor; or ask a colleague on Listserv. Officer Oss could likely access the company's contact information, including email, phone, and address information from the ISP List. The ISP List contains additional information for contacting the appropriate personnel at Nectarine. The critical address for serving legal process on a company providing communication services is the location of the company's corporate headquarters, not the physical location of servers, which is typically unknown to law enforcement. Once received by the company, the preservation letter secures the target data for ninety days, with a possible extension of an additional ninety days.²⁴⁸ Officer Oss may now focus on drafting the appropriate legal process.

In the initial hypothetical, Officer Oss limits her data requests to chats and photographs. Even so, she would be wise to take a much broader view of the potential digital evidence available to her. For example, a subpoena for non-content subscriber information may reveal other Nectarine services John uses, IP addresses, sources of payment, different phone numbers, or email addresses associated with the account. All this information may lead to additional incriminating information, contraband, and other potential corroboration. Nectarine may also retain location information about John's nPhone. Based on the *Carpenter* decision rationale, caution mandates Officer Oss to use a search warrant to request location data. The mere inclusion of slight location information is not necessarily fatal to a subpoena or § 2703(d) order. Yet, the *Carpenter* Court fired a cautionary flare by distinguishing traditional "business records that might incidentally reveal location information" from the CSLI records in *Carpenter*, which included the collection of thousands of data points with location information.²⁴⁹

For brevity's sake, we will focus on the potential chats and photographs. These data types constitute wire or electronic communication content, so Officer Oss should follow the old mantra, "when in doubt, get a

²⁴⁸ 18 U.S.C. § 2703(f)(2) (2018).

²⁴⁹ *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018).

search warrant.” Midgard’s state laws do not prohibit the issuance of SCA warrants to out-of-state entities by one of Midgard’s many courts of competent jurisdiction. While drafting the follow-up legal process to secure account information, Officer Oss should also request delayed notice to the subscriber regarding any request for data. While pursuing this data, Officer Oss should consider statute of limitations issues and tolling options.²⁵⁰

C. *Obtaining Internationally Stored Data via CLOUD Act Agreement*

After her rousing success in the above hypothetical case, Officer Oss transferred to an investigative position in Jotunheim, recently admitted as the fifty-third state. Her first case involved Marv Springstein, who downloaded and compiled an extensive collection of child sexual abuse material. Springstein stored this material in an online cloud account managed by LockBox, a United States corporation. Springstein was extremely careful to avoid storing any information in his digital devices or vehicles. Officer Oss immediately sent a preservation letter to LockBox and followed up with a search warrant issued by a Jotunheim magistrate. LockBox informed Officer Oss that all its servers are in the United Kingdom, outside the United States’ jurisdiction.

1. *Can Officer Oss Access This Information, and if So, How?*

This fact pattern emerges from the circumstances presented in *United States v. Microsoft Corp.*,²⁵¹ where the government sought an SCA warrant to require Microsoft to produce all emails and information associated with an account hosted by Microsoft.²⁵² The CLOUD Act clarified that, subject to exceptions, if the requested data is in the possession or control of a United States corporation, organization, or legal person, SCA warrants must be honored, even if the data is stored overseas.²⁵³

Clearly, Officer Kay Oss is on firm footing in obtaining this data since the United Kingdom is the first nation to enter into a bilateral agreement with the United States, as envisioned by the CLOUD Act.²⁵⁴ Agreements are permissible “only to obtain information relating to . . .

²⁵⁰ See *infra* Section V.D.

²⁵¹ See *supra* Section III.A.; *United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018).

²⁵² *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 829 F.3d 197 (2d Cir. 2016), *vacated and remanded sub nom. Microsoft Corp.*, 138 S. Ct. 1186.

²⁵³ See generally Clarifying Lawful Overseas Use of Data Act, H.R. 4943, 115th Cong. (2018) (enacted), <https://www.justice.gov/dag/page/file/1152896/download> [<https://perma.cc/KQH5-N9QT>] [hereinafter CLOUD Act].

²⁵⁴ *U.S. and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online*, U.S. DEP’T OF JUST. (Oct. 3, 2019), <https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists> [<https://perma.cc/4B5G-FMSK>].

serious crime,” a term that is not defined by the CLOUD Act, aside from noting that “terrorism” is included.²⁵⁵ Fortunately, the United Kingdom bilateral agreement defines “serious crime” as crime that carries “a maximum sentence of at least three (3) years imprisonment.”²⁵⁶ As in the CLOUD Act, no specific crimes are listed aside from terrorism.²⁵⁷ Springstein’s “extensive collection” of child sexual abuse material should meet this threshold. While pursuing this data, Officer Oss should consider statute of limitations issues and tolling options.²⁵⁸

It should be noted that the CLOUD Act “supplements rather than eliminates” MLATs, which remain “another method by which evidence” may be made available.²⁵⁹

One significant change created by the CLOUD Act involved amending the SCA to enable service providers to move to modify or quash SCA warrants. “Court[s] may modify or quash the legal process”²⁶⁰ upon request by providers, if the court determines: (1) that compliance with process would violate the laws of a “qualifying foreign government;”²⁶¹ (2) that modification or quashing is in the interests of justice based on the totality of the circumstances; and (3) that the target of legal process is not a United States person or resident.²⁶² The CLOUD Act also mandates an eight-factor comity analysis in determining the interests of justice.²⁶³

²⁵⁵ THE PURPOSE AND IMPACT OF THE CLOUD ACT, *supra* note 36, at 5.

²⁵⁶ See *supra* Part IV.

²⁵⁷ CLOUD Act, *supra* note 255, at 16.

²⁵⁸ See *infra* Section V.D.

²⁵⁹ THE PURPOSE AND IMPACT OF THE CLOUD ACT, *supra* note 36, at 11.

²⁶⁰ 18 U.S.C. § 2703(h)(2)(B) (2018).

²⁶¹ “Qualifying foreign government” is defined in 18 U.S.C. § 2703(h)(1)(A) (2018) as a foreign government “with which the United States has an executive agreement that has entered into force under” 18 U.S.C. § 2523 (2018). The foreign government must also maintain laws “which provide to electronic communication service providers and remote computing service providers substantive and procedural opportunities similar to those provided” in 18 U.S.C. § 2703(h)(2) (2018) (“Motions to Quash or Modify”) and 18 U.S.C. § 2703(h)(5) (2018) (“Disclosure to Qualifying Foreign Governments”).

²⁶² 18 U.S.C. § 2703(h) (2018) (“Comity Analysis and Disclosure of Information Regarding Legal Process Seeking Contents of Wire or Electronic Communication”).

²⁶³ *Id.* § 2703(h)(3)(A)-(H).

(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

Prosecutors should consider the propriety of formal and informal approaches to these conflict of law scenarios.²⁶⁴

D. Obtaining Internationally Stored Data via Mutual Legal Assistance Treaty (MLAT)

Officer Oss's international investigative endeavors continued when she arrested Marv Springstein's brother, Mark Springstein, who also maintained an extensive collection of child sexual abuse material. Unfortunately, Mark Springstein stored his contraband material in a FireBox account instead of LockBox. FireBox is incorporated in the country of Muspelheim and does not have a bilateral agreement pursuant to the CLOUD Act. Muspelheim maintains a mutual legal assistance treaty (MLAT) with the United States.

*1. Can Officer Oss Access This Information in the Absence of a CLOUD Act Agreement?*²

While Officer Oss is unable to utilize the streamlined CLOUD Act process, she could use the MLAT process. As of 2017, sixty-five countries had entered into MLAT agreements with the United States, and the European Union joined an agreement with the United States establishing mutual legal assistance (MLA) mechanisms with all European Union member states.²⁶⁵ If Officer Oss were uncertain whether the United States had an MLAT with Muspelheim, she could work with her prosecutor to

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.

Id.

²⁶⁴ See THE PURPOSE AND IMPACT OF THE CLOUD ACT, *supra* note 36, at 11–16. Additional options for prosecutors could include “narrowing or modifying a request to avoid the conflict; resolving the conflict through closer inquiry or good-faith negotiation; or making the request under an applicable MLAT.” *Id.* at 16.

²⁶⁵ Mark Rush & Jared Kephart, *Lifting the Veil on the MLAT Process: A Guide to Understanding and Responding to MLA Requests*, K & L GATES (Jan. 20, 2017), <https://www.klgates.com/lifting-the-veil-on-the-mlat-process-a-guide-to-understanding-and-responding-to-mla-requests-01-20-2017/> [<https://perma.cc/U4XS-QLRA>].

contact the Department of Justice's Office of International Affairs (OIA) for clarity.²⁶⁶

The United States Attorney's Manual provides guidance to Officer Oss on the specific steps in submitting a treaty request.²⁶⁷ Because each treaty is negotiated by and with different parties, the treaties' content varies greatly, regardless of the subject matter. As a result, the United States Attorney's Manual explains that OIA will provide prosecutors with model requests based on the specific jurisdiction.²⁶⁸

Based on this model, prosecutors are encouraged to describe "simply and clearly the facts of the case" and "nature of the assistance requested" without using technical legal terms, such as "RICO or even probable cause."²⁶⁹ Since most applications will be translated to local languages, legal terms may or may not have local equivalencies, even if the same legal concepts are utilized.

Prosecutors should then send this draft to OIA, which will either finalize the request or return to the prosecutor for needed changes. The "central authority" of all treaties currently in force is the Department of Justice, which leads to the request being signed in the Department and not by a judge.²⁷⁰ Following signature, translation is arranged, and upon receipt of translation, OIA transmits the MLAT request to the foreign "central authority."²⁷¹

Following receipt of the request, Muspelheim will process the request according to its pertinent domestic law and acquire the necessary court authority to access Mark Springstein's FireBox account. Assuming the Muspelheim judicial system grants the order, then local Muspelheim authorities acquire the resulting data and send it to Officer Oss.²⁷²

The acquired evidence must still pass standard evidentiary thresholds to be admissible in court. Prosecutors should also prospectively consider attempting to toll the relevant statute of limitations when they initiate legal process, given the long time frames often involved in locating and receiving evidence from foreign countries. At the federal level,

²⁶⁶ See U.S. DEP'T OF JUST., JUSTICE MANUAL § 276 (2020), <https://www.justice.gov/archives/jm/criminal-resource-manual-276-treaty-requests> [https://perma.cc/CMT3-X5XZ].

²⁶⁷ *Id.*

²⁶⁸ A sample request is provided in the Appendix.

²⁶⁹ See U.S. DEP'T OF JUST., JUSTICE MANUAL § 281 (2020), <https://www.justice.gov/archives/jm/criminal-resource-manual-281-drafting-requests-assistance> [https://perma.cc/WS5X-HJED]. "RICO" refers to the Racketeer Influenced and Corrupt Organization Act (RICO). See Organized Crime Control Act of 1970, Pub. L. No. 91-452, 84 Stat. 922; 18 U.S.C. § 1961 *et seq.*

²⁷⁰ See JUSTICE MANUAL § 276, *supra* note 268.

²⁷¹ *Id.*

²⁷² See THE PURPOSE AND IMPACT OF THE CLOUD ACT, *supra* note 36, at 3.

prosecutors are empowered to file applications with district courts to suspend the running of the statute of limitations. Applications are granted when the court makes a finding, by a preponderance of the evidence, that the government made an “official request”²⁷³ to obtain foreign evidence, and it “reasonably appears, or reasonably appeared” when the request was made, that the evidence would be found in the foreign country.²⁷⁴ Importantly, the suspension has limited duration.²⁷⁵

E. Obtaining Internationally Stored Data Without MLATs or CLOUD Act Agreements

As Officer Oss’s career continued, she encountered a similar scenario while investigating another distributor of child sexual abuse material, Mike Springstein. Officer Oss’s investigation uncovered significant evidence that Mike’s contraband material is stored on his cloud account within the Icebox social media platform. Icebox is incorporated in Niffelheim, a nation which does not have a CLOUD Act or MLAT agreement with the United States. Prior negotiations over these specific agreements have been unproductive due to diplomatic tension over numerous human rights violations throughout Niffelheim.

1. Does Officer Oss Have Any Legal Process Options in the Absence of Both Agreements?

First, Officer Oss should consider that CLOUD Act and MLAT agreements are not the only categories of relevant international agreements; numerous interim executive agreements exist with several countries.²⁷⁶ Accordingly, Officer Oss should contact the United States OIA to determine what agreements and options may exist to determine optimal instruments and approaches in this geopolitical context.²⁷⁷

²⁷³ “As used in this section, the term ‘official request’ means a letter rogatory, a request under a treaty or convention, or any other request for evidence made by a court of the United States or an authority of the United States having criminal law enforcement responsibility, to a court or other authority of a foreign country.” 18 U.S.C. § 3292(d) (2018).

²⁷⁴ *Id.* § 3292(a)(1).

²⁷⁵ *Id.* § 3292(c) (“The total of all periods of suspension under this section with respect to an offense— (1) shall not exceed three years; and (2) shall not extend a period within which a criminal case must be initiated for more than six months if all foreign authorities take final action before such period would expire without regard to this section.”).

²⁷⁶ U.S. DEP’T OF JUST., JUSTICE MANUAL § 277 (2020), <https://www.justice.gov/archives/jm/criminal-resource-manual-277-executive-agreements-and-memoranda-understanding-mutual-assistance> [<https://perma.cc/W8CK-RQB8>].

²⁷⁷ *Id.*

In all cases, prosecutors must first “determine the jurisdiction from which assistance is needed.”²⁷⁸ Since assistance from foreign jurisdictions typically “depends on the existence of articulable facts,” indicating the evidence’s presence within the foreign jurisdiction, prosecutors should be prepared to state this information.²⁷⁹

Officer Oss should not assume the complete absence of treaties or executive agreements, but even in such a scenario, letters rogatory may provide a solution. A letter rogatory is a request from a US judge to a foreign country’s judiciary, requesting an act which “would constitute a violation of that country’s sovereignty[]”²⁸⁰ if performed without the foreign court’s consent.

While letters rogatory are typically delivered through diplomatic channels, a more efficient method is “by transmitting a copy of the request through Interpol” or other direct route.²⁸¹ A rogatory letter’s form and content varies depending on the recipient country; thus, prosecutors should consult with the United States OIA throughout the drafting process.²⁸² The United States Attorney’s Manual provides helpful procedural steps for letters rogatory.²⁸³ The Department of Justice estimates that the letters

²⁷⁸ U.S. DEP’T OF JUST., JUSTICE MANUAL § 268 (2020), <https://www.justice.gov/archives/jm/criminal-resource-manual-268-location-evidence> [<https://perma.cc/KJ9W-UJXJ>].

²⁷⁹ *Id.*

²⁸⁰ U.S. DEP’T OF JUST., JUSTICE MANUAL § 275 (2020), <https://www.justice.gov/archives/jm/criminal-resource-manual-275-letters-rogatory> [<https://perma.cc/AM26-MQ7P>].

²⁸¹ *Id.*

²⁸² *Id.*

Letters rogatory generally include: (1) background (who is investigating whom and for what charge); (2) the facts (enough information about the case for the foreign judge to conclude that a crime has been committed and to see the relevance of the evidence that is being sought); (3) assistance requested (be specific but include an elastic clause to allow subsequent expansion of the request without filing an additional letter rogatory); (4) the text of the statutes alleged to have been violated; and (5) a promise of reciprocity. Letters rogatory must be signed by a judge and, normally, authenticated by (1) an apostille, (2) an exemplification certificate, (3) a chain certificate of authentication, or (4) as directed by OIA. If the requested state has ratified the Hague Convention Abolishing the Requirement of Legalization of Foreign Public Documents, it is preferable to use an apostille. The chain certification is a cumbersome process involving authentication by the Department of Justice, the Department of State, and the embassy of the foreign country to which the letter rogatory is directed. Consult OIA to ascertain which method to use because authentication requirements change frequently.

Id.

²⁸³ *Id.*

rogatory method of assistance can take a year or more,²⁸⁴ so prosecutors should strongly consider statute of limitations issues and tolling options in this context.²⁸⁵

Officer Oss could also attempt various “informal means” of obtaining evidence from Niffelheim, though she should recognize that some methods may not yield admissible evidence.²⁸⁶ These could include asking foreign authorities to open an investigation and share evidence; requesting that foreign jurisdictions provide public records to United States law enforcement; conducting “depositions of voluntary witnesses”²⁸⁷ at United States embassies and consulates; making treaty requests; using informal requests between law enforcement agencies; and sending requests through Interpol for evidence or information.²⁸⁸

The Convention on Cybercrime, or “Budapest Convention,” is a critical international agreement that has been ratified by sixty-five countries

First, obtain a model from OIA [Office of International Affairs] and check with OIA to ascertain the requirements of the particular country. Second, prepare a draft . . . and send it to OIA for clearance. Third, secure a judge’s signature. Submit the cleared final to the district court in two originals under cover of an application for issuance of letters rogatory and a memorandum in support, models of which have been obtained from OIA. One signed original letter rogatory remains with the court. Fourth, authenticate as directed by OIA. Unless OIA has instructed you differently, affix an apostille or other authentication to the signed duplicate original and send it and two copies to OIA. Fifth, make arrangements for translation . . . and send the duplicate original with translation to OIA, which will transmit it to the Department of State, the American Embassy in the country concerned, or directly to the appropriate ministry or authority in the country concerned. If OIA transmits the letter rogatory with translation via the diplomatic channel, the Embassy will send it to the Foreign Ministry under cover of a diplomatic note, the Foreign Ministry will usually refer it to the Ministry of Justice, and the Ministry of Justice will usually forward it to the proper judicial authority where it will be executed. Normally, the evidence, once obtained, is returned through the same channel by which the request was transmitted. In some cases, the request is sent to an attorney in the foreign jurisdiction who is retained to present the request, obtain the evidence, and deliver it to the United States.

Id.

²⁸⁴ *Id.*

²⁸⁵ See *supra* Section V.D.

²⁸⁶ U.S. DEP’T OF JUST., JUSTICE MANUAL § 274 (2020), <https://www.justice.gov/archives/jm/criminal-resource-manual-274-methods> [<https://perma.cc/YFS5-GXZ5>].

²⁸⁷ U.S. DEP’T OF JUST., JUSTICE MANUAL § 278 (2020), <https://www.justice.gov/archives/jm/criminal-resource-manual-278-informal-means> [<https://perma.cc/A78T-CH6R>].

²⁸⁸ *Id.* (referencing current known locations or suspect photographs).

as of April 2020.²⁸⁹ The prolific adoption of the Budapest Convention is cause for optimism by Officer Oss, particularly if Niffelheim is a signatory, since all parties are required to adopt domestic law “under which relevant authorities can compel providers in their territory to disclose electronic data in their possession or control.”²⁹⁰ Even so, the Budapest Convention does not include an exception for “data that a company controls but chooses to store abroad.”²⁹¹

F. *Legal Implications of Extraterrestrial Data Storage*

Data storage—and even the provision of internet service itself—is increasingly explored in the context of satellites. For example, SpaceX has launched over 700 StarLink satellites and obtained approval for 12,000 satellites.²⁹² This phenomenon is so prevalent; optical and radio astronomers are concerned because of satellites’ obstruction of telescopes.²⁹³

Several private entities have entered the industry of space-based data storage.²⁹⁴ SpaceBelt describes itself as a “Cloud Constellation Corporation” that is “leading the cloud transformation of space.”²⁹⁵ SpaceBelt offers increases in data security and convenience as selling points.²⁹⁶ Some companies anticipate energy benefits because solar radiation

²⁸⁹ Convention on Cybercrime, Council of Europe, Nov. 23, 2001, E.T.S. No. 185, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?docId=0900001680081561> [<https://perma.cc/CL23-Z238>]. The official list of party countries is available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=cmPs1otx [<https://perma.cc/7PS5-8AKB>].

²⁹⁰ THE PURPOSE AND IMPACT OF THE CLOUD ACT, *supra* note 36, at 7; *see* Convention on Cybercrime, *supra* note 291, at 9 (mandating each signatory to “adopt such legislative and other measures as may be necessary to empower its competent authorities to order . . . a person in its territory to submit specified computer data in that person’s possession or control, which is stored in a computer system or a computer-data storage medium”).

²⁹¹ THE PURPOSE AND IMPACT OF THE CLOUD ACT, *supra* note 36, at 7.

²⁹² Daniel Clery, *Starlink Already Threatens Optical Astronomy. Now, Radio Astronomers Are Worried*, SCI. (Oct. 9, 2020, 2:25 PM), <https://www.sciencemag.org/news/2020/10/starlink-already-threatens-optical-astronomy-now-radio-astronomers-are-worried> [<https://perma.cc/8ULK-NUBH>].

²⁹³ *Id.*

²⁹⁴ *See generally* Yevgeniy Sverdlik, *Space: The Ultimate Network Edge*, DATACENTER KNOWLEDGE (Oct. 17, 2016), <https://www.datacenterknowledge.com/archives/2016/10/17/space-the-ultimate-network-edge> [<https://perma.cc/5QY7-82WW>]; SPACEBELT, <http://spacebelt.com/#about> [<https://perma.cc/TX2F-K5LX>]; CONNECTX, <https://connectx.com/> [<https://perma.cc/E9TA-U2QT>].

²⁹⁵ SPACEBELT, *supra* note 296.

²⁹⁶ *Id.*

could power servers at a minimal cost.²⁹⁷ Space itself may provide practical advantages for data storage since “the cold of space could allow faster processing without the risk of overheating.”²⁹⁸ Some predict significant cost savings given the proliferation of terrestrial data centers,²⁹⁹ the economic costs of cybersecurity maintenance and breaches of terrestrial infrastructure,³⁰⁰ and the decreasing costs of launching satellites into orbit.³⁰¹

Extraterrestrial data storage also provides context for additional innovation in data delivery. For example, machine learning models can predict the best routes for data transmission:

If you are located in Emeryville, California . . . and it’s a cloudy day in the Bay Area, the system will not send the signal [from space] directly to Emeryville. Instead, it may drop it down further south, say in Sacramento, where the sky is clear and from where the data will be routed along terrestrial fiber to its intended recipient[.]³⁰²

Returning to the hypothetical, let us assume that Officer Oss opens an investigation of Joe Collector, an eccentric, independently wealthy billionaire who maintains various exotic flora and fauna in an increasingly crowded menagerie. Aside from discovering numerous Endangered Species Act violations, Officer Oss developed probable cause to believe that Joe stores another collection of illegal images and videos on a satellite currently in Earth’s orbit. At the time Officer Oss sought a search warrant, the satellite was in orbit directly above the sovereign nation of Paradise Archipelago. Infinity Dust, Inc. launched and maintained the satellite, which is based in Midgard, the nation where Oss currently serves as a law enforcement officer. When Officer Oss arrested Joe, he was not overly concerned. Instead, Joe bragged about how he stores the data in outer space—safely beyond the jurisdiction of any terrestrial government.

²⁹⁷ Rick Delgado, *Cloud Computing Is Moving to Outer Space?*, SMARTDATA COLLECTIVE (June 21, 2016), <https://www.smartdatacollective.com/cloud-computing-moving-outer-space/> [https://perma.cc/LEK9-YVZD].

²⁹⁸ *Id.*

²⁹⁹ Dan Matthews, *Data Storage in Space? It’s Already in the Works*, SMARTDATA COLLECTIVE (Apr. 2, 2018), <https://www.smartdatacollective.com/data-storage-space-works/> [https://perma.cc/Q3VR-75JX].

³⁰⁰ Michael Sheetz, *Satellite Start-Up Raises \$100 Million to Put Cloud Data Storage in Space*, CNBC (Dec. 20, 2018), <https://www.cnbc.com/2018/12/19/cloud-constellation-raises-100-million-to-store-cloud-data-in-space.html> [https://perma.cc/4WZL-Z9NL].

³⁰¹ Delgado, *supra* note 299.

³⁰² Sverdlik, *supra* note 296.

1. *Can Officer Oss Access Joe Collector's Data, Despite its Location in Outer Space?*

This hypothetical provides an additional illustration of the importance of focusing on the physical location of the corporation maintaining the data, as opposed to the actual physical location of the targeted data.³⁰³ The satellite's orbital location above Paradise Archipelago is irrelevant since the servers' location—terrestrial or extraterrestrial—is not the dispositive consideration for legal process. Rather, Officer Oss should direct her attention to the corporation maintaining the relevant data, which is in Midgard. An immediate preservation letter should be sent, followed by a search warrant.

Extraterrestrial data storage implications may receive judicial attention in the near future. While the hypothetical based on extraterrestrial data storage seems inconceivable, a few entities already marketed extraterrestrial data storage to conceal data from governmental actors. For example, one extraterrestrial data storage corporation advertises that “no one can physically access our [satellite] system and no government or entity can force the exposure of your information.”³⁰⁴ Asgardia—a company based out of Vienna, Austria—styles itself as the first space-based nation. It possesses its own calendar, constitution, parliament, national symbols, and, as of November 2017, its own satellite with data storage capabilities, seeking to store data “beyond the reach of Earthly laws.”³⁰⁵ While it is beyond this Article's scope to explore international law issues presented by these arguments,³⁰⁶ numerous pertinent international law sources and oversight have existed since the birth of space exploration.³⁰⁷

³⁰³ See *supra* Section V.B.

³⁰⁴ Andrew Donoghue, *The Idea of Data Centers in Space Just Got a Little Less Crazy*, DATA CENTER KNOWLEDGE (Feb. 9, 2018), <https://www.datacenterknowledge.com/edge-computing/idea-data-centers-space-just-got-little-less-crazy> [https://perma.cc/Y9HJ-JDHR].

³⁰⁵ Mark Harris, *The First Space-Based 'Nation' Wants to Store Data Off-Planet, Beyond the Law*, VICE (June 6, 2017), <https://www.vice.com/en/article/a3zveg/asgardia-nation-space-data-storage-off-planet> [https://perma.cc/BKS5-39GW]. Asgardia purports to be a non-governmental organization based in Vienna, Austria. ASGARDIA THE SPACE NATION, <https://asgardia.space/en/page/imprint> [https://perma.cc/H7HG-UQJ2].

³⁰⁶ Convention on Cybercrime, *supra* note 291.

³⁰⁷ See Yun Zhao, *Space Commercialization and the Development of Space Law*, OXFORD RSCH. ENCYC. PLANETARY SCI. (July 30, 2018), <https://oxfordre.com/planetariscience/view/10.1093/acrefore/9780190647926.001.0001/acrefore-9780190647926-e-42> [https://perma.cc/X2PC-M9ZJ].

VI. APPENDIX³⁰⁸*A. Long-Arm Statutes*³⁰⁹**Alabama:**

ALA. R. CIV. P. 4.2 (Westlaw through Nov. 20, 2020); *Butler v. Beer Across America*, 83 F. Supp. 2d 1261 (N.D. Ala. 2000); *Keelean v. Cent. Bank of the South*, 544 So. 2d 153 (Ala. 1989), *overruled by Prof'l Ins. Corp. v. Sutherland*, 700 So. 2d 347 (Ala. 1997)).

Alaska:

ALASKA STAT. § 09.05.015 (West, Westlaw through Chapter 32 and Ballot Measure 2 of the 2020 Second Reg. Sess. of the 31st Leg.); *Kenecorp Mortg. & Equities, Inc. v. First Nat'l Bank of Fairbanks*, 685 P.2d 1232 (Ala. 1984).

Arizona:

ARIZ. R. CIV. P. 4.2 (Westlaw through Jan. 1, 2021); *Aries v. Palmer Johnson, Inc.*, 735 P.2d 1373 (Ariz. Ct. App. 1987); *Meyers v. Hamilton Corp.*, 693 P.2d 904 (Ariz. 1985).

Arkansas:

ARK. CODE ANN. § 16-4-101 (West, Westlaw through Dec. 15, 2020); *Pennsalt Chem. Corp. v. Crown Cork & Seal Co.*, 426 S.W.2d 417 (Ark. 1968); *Smith v. Hobby Lobby Stores, Inc.*, 968 F. Supp. 1356 (W.D. Ark. 1997).

California:

CAL. CODE CIV. P. § 410.10 (West, Westlaw through Chapter 13 of 2021 Reg. Sess); *Abbott Power Corp. v. Overhead Elec. Co.*, 131 Cal. Rptr. 508 (Cal. Ct. App. 1976); *Pavlovich v. Superior Court*, 58 P.3d 2 (Cal. 2002).

Colorado:

COLO. REV. STAT. § 13-1-124 (West, Westlaw through Mar. 16, 2021); *Waterval v. District Court In & For El Paso County*, 620 P.2d 5 (Colo. 1980).

Connecticut:

CONN. GEN. STAT. § 52-59b (West, Westlaw through Mar. 4, 2021); *Gates v. Royal Palace Hotel*, 23 Conn. L. Rptr. 670 (Conn. Super. Ct. Dec. 30, 1998); *Standard Tallow Corp. v. Jowdy*, 459 A.2d 503 (Conn. 1983).

³⁰⁸ Numerous templates for prosecutors, law enforcement officers, and allied professionals are available on the National White-Collar Crime Center (NW3C) and Zero Abuse Project websites. See NW3C, INC., nw3c.org [https://perma.cc/TH7X-4XZZ], and ZERO ABUSE PROJECT, zeroabuseproject.org [https://perma.cc/5JNY-E5EX] for more information. These templates include sample letters of preservation, search warrants and related affidavits, and MLAT requests, among other resources.

³⁰⁹ See *Long-Arm Statutes: A Fifty-State Survey*, VEDDER PRICE (2003), <http://euro.ecom.cmu.edu/program/law/08-732/Jurisdiction/LongArmSurvey.pdf> [https://perma.cc/JWR7-RWHK].

Delaware:

DEL. CODE ANN. tit. 10, § 3104 (West, Westlaw through Chapter 7 of the 151st Gen. Assemb. (2021-2022)); *Eudaily v. Harmon*, 420 A.2d 1175 (Del. 1980); *Kane v. Coffman*, No. 00C-08-236, 2001 WL 914016 (Del. Super. Ct. 2001).

District of Columbia (D.C.):

D.C. CODE § 13-423 (West, Westlaw through Feb. 3, 2021); *Env't Rsch. Int'l, Inc. v. Lockwood Greene Eng'rs, Inc.*, 355 A.2d 808 (D.C. 1975); *GTE New Media Servs., Inc. v. Ameritech Corp.*, 44 F. Supp. 2d 313 (D.D.C. 1999).

Florida:

FLA. STAT. § 48.193 (West, Westlaw through the 2020 Second Reg. Sess. of the 26th Leg.); *Homeway Furniture Co. of Mount Airy, Inc. v. Home*, 822 So. 2d 533 (Fla. Dist. Ct. App. 2002).

Georgia:

GA. CODE ANN. § 9-10-91 (2003) (West, Westlaw through 2021, Act 4); *Beasley v. Beasley*, 396 S.E.2d 222 (Ga. 1990).

Hawaii:

HAW. REV. STAT. § 634-35 (West, Westlaw through Act 1 of the 2021 Reg. Sess.); *Cowan v. First Ins. Co. of Hawaii, LTD.*, 608 P.2d 394 (Haw. 1980).

Idaho:

IDAHO CODE § 5-514 (West, Westlaw through Jan. 11, 2021); *Schneider v. Sverdsten Logging Co.*, 657 P.2d 1078 (Idaho 1983).

Illinois:

735 ILL. COMP. STAT. 5/2-209 (Westlaw through P.A. 101-655); *Aero Products Int'l, Inc. v. Intex Corp.*, No. 02 C 2590, 2002 U.S. Dist. LEXIS 17948 (N.D. Ill. 2002); *Baltimore & Ohio R.R. Co. v. Mosele*, 368 N.E.2d 88 (Ill. 1977).

Indiana:

IND. R. TRIAL P. 4.4 (Westlaw through Jan. 15, 2021); *Anthem Ins. Cos. v. Tenent Healthcare Corp.*, 730 N.E.2d 1227 (Ind. 2000); *Communications Depot, Inc. v. Verizon Commc'ns, Inc.*, No. IP01-1587-C-H/K, 2002 WL 1800044 (S.D. Ind. 2002); *Search Force, Inc. v. Dataforce Int'l, Inc.*, 112 F. Supp. 2d 771 (S.D. Ind. 2000).

Iowa:

IOWA CODE § 617.3 (West, Westlaw through Mar. 8, 2021); *Universal Coops., Inc. v. Tasco, Inc.*, 300 N.W.2d 139 (Iowa 1981).

Kansas:

KAN. STAT. ANN. § 23-36, 210 (West, Westlaw through 2021 Reg. Sess.); *D.J.'s Rock Creek Marina, Inc. v. Imperial Foam & Insulation Mfg. Co.*, No. 01-4139-JAR, 2003 WL 262495 (D. Kan. 2003); *Woodring v. Hall*, 438 P.2d 135 (Kan. 1968).

Kentucky:

KY. REV. STAT. ANN. § 454.210 (West, Westlaw through Chapter 60 of the 2021 Reg. Sess.); *Auto Channel, Inc. v. Speedvision Network, LLC*, 995 F. Supp. 761 (W.D. Ky. 1997); *Tube Turns Div. of Chemtron Corp. v. Patterson Co.*, 562 S.W.2d 99 (Ky. Ct. App. 1978).

Louisiana:

LA STAT. ANN. § 13:320 (Westlaw through 2020 Second Extraordinary Sess.); *Mid City Bowling Lanes & Sports Palace, Inc. v. Ivercrest, Inc.*, 35 F. Supp. 2d 507 (E.D. La. 1999); *Petrol. Helicopters, Inc. v. AVCO Corp.*, 513 So. 2d 1188 (La. 1987).

Maine:

ME. STAT. tit. 14, § 704-A (Westlaw through the 2019 Second Reg. Sess. of the 129th Leg.); *Talarico v. Marathon Shoe Co.*, No. CIV 00-239-P-C, 2001 WL 366346 (D. Me. 2001); *Tyson v. Whitaker & Son, Inc.*, 407 A.2d 1 (Me. 1979).

Maryland:

MD. CODE ANN., COURTS & JUDICIAL PROCEEDINGS § 6-103 (West, Westlaw through Mar. 14, 2021); *A. F. Briggs Co. v. Starrett Corp.*, 329 A.2d 177 (Me. 1974); *ALS Scan, Inc. v. Wilkins*, 142 F. Supp. 2d 703 (D. Md. 2001).

Massachusetts:

MASS. GEN. LAWS ch. 223A, § 3 (West, Westlaw through February 15, 2021); *Back Bay Farm, LLC v. Collucio*, 230 F. Supp. 2d 176 (D. Mass. 2002); *Tatro v. Manor Care, Inc.*, 625 N.E.2d 549 (Mass. 1994).

Michigan:

MICH. COMP. LAWS § 600.705 (West, Westlaw through P.A.2021, No. 3, of the 2021 Reg. Sess.); *Green v. Wilson*, 565 N.W.2d 813 (Mich. 1997); *Siebellink v. Cyclone Airsports, Ltd.*, No. 1:01-CV-591, 2001 WL 1910560 (W.D. Mich. 2001); *Sifers v. Horen*, 188 N.W.2d 623 (Mich. 1971); *Sports Auth. Michigan, Inc. v. Justballs, Inc.*, 97 F. Supp. 2d 806 (E.D. Mich. 2000).

Minnesota:

MINN. STAT. § 543.19 (2003); *State Farm Mut. Auto Ins. Co. v. Tennessee Farmers Mut. Ins. Co.*, 646 N.W.2d 169 (Minn. Ct. App. 2002); *State by Humphrey v. Granite Gate Resorts, Inc.*, 568 N.W.2d 715 (Minn. Ct. App. 1997).

Mississippi:

MISS. CODE ANN. § 13-3-57 (West, Westlaw through Mar. 16, 2021); *Internet Doorway, Inc. v. Parks*, 138 F. Supp. 2d 773 (S.D. Miss. 2001); *Mladinich v. Kohn*, 164 So. 2d 785 (Miss. 1964).

Missouri:

MO. REV. STAT. § 506.500 (West, Westlaw through the end of the 2020 Second Reg. Sess. and First and Second Extraordinary Sess. of the 100th Gen. Assemb.); *State ex rel. Deere & Co. v. Pinnell*, 454 S.W.2d 889 (Mo.

1970); *State ex rel. Nixon v. Beer Nuts, Ltd.*, 29 S.W.3d 828 (Mo. Ct. App. 2000).

Montana:

MONT. R. CIV. P. 4B (Westlaw through Feb. 18, 2021); *Bedrejo v. Triple E Canada, Ltd.*, 984 P.2d 739 (Mont. 1999); *Simmons v. State*, 670 P.2d 1372 (Mont. 1983).

Nebraska:

NEB. REV. STAT. § 25-536 (West, Westlaw through Mar. 18, 2021); *Stucky v. Stucky*, 185 N.W.2d 656 (Neb. 1971); *Wagner v. Unicord Corp.*, 526 N.W.2d 74 (Neb. 1995).

Nevada:

NEV. REV. STAT. § 14.065 (West, Westlaw Chapter 3 of the 81st Reg. Sess.); *Certain-Teed Prod. Corp. v. Second Judicial District Court*, 479 P.2d 781 (Nev. 1971); *Graziose v. Am. Home Prods. Corp.*, 161 F. Supp. 2d 1149 (D. Nev. 2001); *Trump v. Eighth Judicial District Court (Becker)*, 857 P.2d 740 (Nev. 1993).

New Hampshire:

N.H. REV. STAT. ANN. § 510:4 (Westlaw through 2020 Reg. Sess. of the Gen. Ct.); *Estabrook v. Wetmore*, 529 A.2d 956 (N.H. 1987); *Phelps v. Kingston*, 536 A.2d 740 (N.H. 1987); *Metcalf v. Lawson*, 802 A.2d 1221 (N.H. 2002); *Remsbury v. Docusearch, Inc.*, No. CIV. 00-211-B, 2002 WL 130952 (D.N.H. Jan. 31, 2002).

New Jersey:

N.J. CT. R. R. 4:4-4 (Westlaw through Feb. 1, 2021); *Avdel Corp. v. Mecure*, 277 A.2d 207 (N.J. 1971); *Gendler & Co. v. Telecom Equip. Corp.*, 508 A.2d 1127 (N.J. 1986); *Ragonese v. Rosenfeld*, 722 A.2d 991 (N.J. Super. Ct. 1998).

New Mexico:

N.M. STAT. ANN. § 38-1-16 (West, Westlaw through Chapter 6 of the 1st Reg. Sess. of the 55th Leg.); *Origins Nat. Res., Inc. v. Kotler*, 133 F. Supp. 2d 1232 (D.N.M. 2001); *Telephonic, Inc. v. Rosenblum*, 543 P.2d 825 (N.M. 1975); *Windward v. Holly Creek Mills, Inc.*, 493 P.2d 954 (N.M. 1972).

New York:

N.Y. C.P.L.R. 302 (McKinney, Westlaw through L.2021, Chapters 1 to 49, 61 to 80); *Armouth Int'l, Inc. v. Haband Co.*, 715 N.Y.S.2d 438 (N.Y. App. Div. 2000); *Longines-Witnauer Watch Co. v. Barnes & Reinecke, Inc.*, 209 N.E.2d 68 (N.Y. 1965).

North Carolina:

N.C. GEN. STAT. § 1-75.4 (Westlaw through the end of the 2020 Reg. Sess. of the Gen. Assemb.); *Dillon v. Numismatic Funding Corp.*, 231 S.E.2d 629 (N.C. 1977); *Replacements, Ltd. v. MidweSterling*, 515 S.E.2d 46 (N.C. Ct. App. 1999).

North Dakota:

N.D. R. Civ. P. 4 (Westlaw through January 15, 2021); *Hebron Brick Co. v. Robinson Brick & Tile Co.*, 234 N.W.2d 250 (N.D. 1975).

Ohio:

OHIO REV. CODE ANN. § 2307.382 (West, Westlaw through Files 1 to 115 of the 133rd Gen. Assemb.); *CompuServe, Inc. v. Patterson*, 89 F.3d 1257 (6th Cir. 1996); *U.S. Sprint Commc'ns Co. P'ship v. Mr. K's Foods, Inc.*, 624 N.E.2d 1048 (Ohio 1994).

Oklahoma:

OKLA. STAT. tit. 12, § 2004 (West, Westlaw through Chapter 2 of the First Reg. Sess. of the 58th Leg.); *Hough v. Leonard*, 867 P.2d 438 (Okla. 1993); *Intercon, Inc. v. Bell Atl. Internet Sols., Inc.*, 205 F.3d 1244 (10th Cir. 2000).

Oregon:

OR. R. Civ. P. 4 (Westlaw through Mar. 3, 2020); *State, ex rel. Hydraulic Servocontrols Corp. v. Dale*, 657 P.2d 211 (Or. 1982); *Tech Heads, Inc. v. Desktop Serv. Ctr., Inc.*, 105 F. Supp. 2d 1142 (D. Or. 2000).

Pennsylvania:

42 PA. STAT. AND CONS. STAT. ANN. § 5322 (West, Westlaw through 2021 Reg. Sess. Act 9); *Kenny v. Alexson Equip. Co.*, 432 A.2d 974 (Pa. 1981); *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997).

Puerto Rico:

P.R. LAWS ANN. tit. 32A, § III, R. 4.7 (2019); *Pou v. Am. Motors Corp.*, 127 P.R. Dec. 810 (P.R. 1991).

Rhode Island:

9 R.I. GEN. LAWS § 9-5-33 (West, Westlaw through Jan. 7, 2020); *Conn v. ITT Aetna Fin. Co.*, 252 A.2d 184 (R.I. 1969).

South Carolina:

S.C. CODE ANN. § 36-2-803 (Westlaw through 2021 Act No. 7); *Sheppard v. Jacksonville Marine Supply, Inc.*, 877 F. Supp. 260 (D.S.C. 1995).

South Dakota:

S.D. CODIFIED LAWS § 15-7-2 (Westlaw through Mar. 22, 2021); *Ventling v. Kraft*, 161 N.W.2d 29 (S.D. 1968).

Tennessee:

TENN. CODE ANN. § 20-2-214 (West, Westlaw through Feb. 3, 2021); *Bailey v. Turbine Design, Inc.*, F. Supp. 2d 790 (W.D. Tenn. 2000); *Masada Inv. Corp. v. Allen*, 697 S.W.2d 332 (Tenn. 1985).

Texas:

TEX. CIV. PRAC. & REM. CODE ANN. § 17.042 (West, Westlaw through end of the 2019 Reg. Sess. of the 86th Leg.); *Riviera Operating Corp. v. Dawson*, 29 S.W.3d 905 (Tex. Civ. App. 2000); *U-Anchor Advert., Inc. v. Burt*, 553 S.W.2d 760 (Tex. 1977).

Utah:

UTAH CODE ANN. 1953 § 78-27-24, *renumbered as* § 78B-3-205 (West through 2020 6th Spec. Sess.); *Brown v. Carnes Corp.*, 611 P.2d 378 (Utah 1980); *iAccess, Inc. v. WEBcard Techs., Inc.*, 182 F. Supp. 2d 1183 (D. Utah 2002).

Vermont:

VT. STAT. ANN. tit. 12, §§ 855, 913 (West, Westlaw through Acts 1 through 4 of the Reg. Sess. of the 2021–2022 Vt. Gen. Assemb.); *Bard Bldg. Supply Co. v. United Foam Corp.*, 400 A.2d 1023 (Vt. 1979); *O'Brien v. Comstock Foods, Inc.*, 194 A.2d 568 (Vt. 1963).

Virginia:

VA. CODE ANN. § 8.01-328.1 (West, Westlaw through the End of 2021 Reg. Sess.); *Alitalia-Linee Aeree Italiane S.p.A. v. Casinoalitalia.Com*, 128 F. Supp. 2d 340 (E.D. Va. 2001); *Carmichael v. Snyder*, 164 S.E.2d 703 (Va. 1968); *Verizon Online Servs., Inc. v. Ralsky*, 203 F. Supp. 2d 601 (E.D. Va. 2002).

Washington:

WASH. REV. CODE § 4.28.185 (West, Westlaw through Chapter 8 of the 2021 Reg. Sess. of the Wash. Leg.); *Precision Lab. Plastics v. Micro Test, Inc.*, 981 P.2d 454 (Wash. Ct. App. 1999); *Tyce Constr. Co. v. Dulien Steel Prods., Inc., of Washington*, 381 P.2d 245 (Wash. 1963).

West Virginia:

W. VA. CODE § 56-3-33 (West, Westlaw through Mar. 16, 2021); *Abbott v. Owens-Corning Fiberglas Corp.*, 444 S.E.2d 285 (W.Va. 1994).

Wisconsin:

WIS. STAT. § 801.05 (West, Westlaw through Apr. 18, 2020); *PKWare, Inc. v. Timothy L. Meade*, 79 F. Supp. 2d 1007 (E.D. Wis. 2000); *Zerbel v. H.L. Federman & Co.*, 179 N.W.2d 872 (Wis. 1970).

Wyoming:

WYO. STAT. ANN. § 5-1-107 (West, Westlaw through Chapters 1–3 of the 2020 Spec. Sess. of the Wyo. Leg.); *First Wyoming Bank, N.A., Rawlins v. Trans Mountain Sales & Leasing, Inc.*, 602 P.2d 1219 (Wyo. 1979).