a program of zero abuse PROJECT

Exigency and Encrypted Cloud Accounts (Part 1)

8 Introductory Considerations for Prosecutors

By Robert J. Peters, Christa Miller, Kathleen Nolan, Caralea Grant, & Lauren Munday

Scenario

Police are called to the residence of Rafael Montoya, whose daughter Graciela has gone missing. Graciela's younger sister tells Detective Marla Rhue that Graciela went to meet her new boyfriend. Rafael has the password to Graciela's iPhone, and grants Det. Rhue access. There, she finds:

- WhatsApp, Snapchat, and Instagram apps with at least a dozen contacts in each and numerous private messages.
- An app, "T-Gram," installed with just a single contact name, "K.S." No messages are stored in the app, and investigators see that "disappearing messages" are enabled, set to 5 minutes. Graciela's sister confirms that the name in the T-Gram app matches what Graciela told her about her boyfriend.
- Screenshots, stored locally, of messages between Graciela and K.S. going back two months. Many of the messages are sexually explicit.
- Some of the messages refer to videos, though investigators can find none stored on the device nor in Graciela's iCloud account. Most recently, however, there are threats: K.S. has told her he's stored the videos on a cloud server known as "Massiv" and "it would be nothing" for him to forward the links to Graciela's family and friends if she doesn't do what he says.

Encryption and remotely stored data have become ubiquitous in criminal investigations, yet the Stored Communications Act (SCA) prescribes limited methods for accessing such evidence. As a result, prosecutors and investigators increasingly encounter situations where exigent circumstances, cloud accounts, and encryption coalesce—making vital information inaccessible with a normal search warrant. "Exigency and Encrypted Cloud Accounts" helps prosecutors better understand these data access issues and strategize solutions for apparent no-win scenarios. Part 1, below, offers eight introductory considerations for prosecutors dealing with exigency and encrypted cloud accounts, while Part 2 addresses more advanced strategies for dealing with cloud providers and other stakeholders.[1]

[1] Robert J. Peters, Christa Miller, Joseph D. Remy, & Kathleen Nolan, "Exigency and Encrypted Cloud Accounts, Part 2: 7 Advanced Strategies for Prosecutors," ZERO ABUSE PROJECT (2022).

As defined by the 9th Circuit, exigent circumstances are "those circumstances that would cause a reasonable person to believe that [warrantless] entry (or other relevant prompt action) was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts."[2]

In any investigation, the destruction of relevant evidence is highly problematic. However, the risk of destruction increases with digital data—which makes up the bulk of child exploitation evidence—particularly when it is stored in the cloud. The loss of this evidence—such as a media file's geolocation or other identifying information known as metadata—can frustrate efforts to rescue child victims as well as apprehend offenders. Data loss can happen routinely, as part of cloud-service providers' scheduled maintenance. Or it can be targeted, like when offenders remotely wipe (or destroy) evidence from a device no longer in their possession. Methods of exploitation themselves are often selected to minimize trails of digital evidence, such as the live streaming of abuse, which often ends without a file being saved to digital storage media.

Increasingly, data encryption is heightening the risk of exigency as well by slowing or blocking investigators' access to important case information and evidence. Implemented by technology providers in the name of user privacy, data encryption can be applied across the device or for particular portions of data. For instance:

- Full disk encryption can be implemented on a computer or mobile device.
- Users can rely on apps to encrypt certain data they store on a device—even if the rest of the device remains unencrypted—or communications between themselves and another party.
- Electronic service providers can encrypt data stored on their cloud servers or as part of their messaging services.

Because users access their cloud-based data through their computers, mobile phones, tablets, and other devices, the interplay of encrypted data can further complicate law enforcement investigations. Within the bounds of the Stored Communications Act, in particular, little guidance exists for investigators seeking to obtain cloud-based data that's accessible from an encrypted device—especially when the data is also encrypted in the cloud and the provider doesn't maintain the decryption key. Add to this mix service providers and cloud storage in countries outside the United States, and the situation gets complicated. As a result, it is often wise, even when exigent circumstances exist, to obtain a search warrant that clearly articulates probable cause to search.

Follow along with the case scenario above as it tracks eight introductory considerations for prosecutors dealing with possible data preservation, access, and encryption issues under exigent circumstances in their child protection efforts.

---

[2] *United States v. McConney*, 728 F.2d 1195, 1199 (9th Cir. 1984) (overruled on other grounds by *Maric v. Alvarado*, 748 Fed. Appx. 747 (9th Cir. 2018)).

Important Definitions for Terms Related to Remotely Stored Data and Exigent Circumstances	
Biometrics	Biometrics are a person's unique physical characteristics that can be used for automatic recognition.[3] These features may include, but are not limited to, a person's fingerprints, iris pattern, and general facial structure.
Cell Tower Dump; **Cell Site Location Information**	A cell tower dump is the act of accessing the cell phone records of all cell phone users that were within a certain geographical area within a certain period of time. Cell networks track both a user's location and time whenever a user accesses their cell phone; this information, also known as cell site location information (CSLI) is stored with service providers for multiple years and can be accessed by willing providers or with a search warrant.[4]
Cloud/Cloud Accounts	Per *Cloudflare.com*, the cloud is defined as "servers that are accessed over the [i]nternet, and the software and databases that run on those servers. Cloud servers are located in data centers all over the world. By using cloud computing, users and companies don't have to manage physical servers themselves or run software applications on their own machines. The cloud enables users to access the same files and applications from almost any device, because the computing and storage takes place on servers in a data center, instead of locally on the user device."[5]
Data	Data here refers to the "quantities, characters, or symbols on which operations are performed by a computer, being stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media."[6]
Encryption	Encryption, in its most basic sense, is a security mechanism that takes data protection a step further than concealing it behind a password. Instead, encryption scrambles data via a cipher, or code. An encryption scheme converts plain text to unreadable ciphertext; to convert the text back from ciphertext to plain text, a key is needed. The key can be: • A bodily characteristic, such as a fingerprint, voice, or face • A password, phrase, or code (that doesn't merely protect access to data) • An automatically generated key • A partial password or a partial automatically generated key

[3] DEPARTMENT OF HOMELAND SECURITY, BIOMETRICS (2021), https://www.dhs.gov/biometrics.
[4] Mason Kortz & Christopher Bavitz, Cell Tower Dumps, Bos. Bar J. (Mar. 18, 2019), https://bostonbarjournal.com/2019/03/18/cell-tower-dumps/.
[5] CLOUDFLARE, https://www.cloudflare.com/learning/cloud/what-is-the-cloud/ (last visited July 19, 2021).
[6] Data, OXFORD LANGUAGES DICTIONARY (3d ed. 2020).

	• Any of these combined (multi-factor authentication, or MFA)
Forensic Artifact **(Digital Evidence)**	Forensic artifacts are digital traces of the user's behavior that amount to evidence, including (but not limited to) time stamps, entry files, registry keys, or files.[7]
Geofencing	Geofencing refers to the "use of GPS or RFID technology to create a virtual geographic boundary, enabling software to trigger a response when a mobile device enters or leaves a particular area."[8]
IP Address	An "Internet Protocol Address," or IP address, is a "numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: host or network interface identification and location addressing."[9]
Lawful Hacking	"Also known as 'government hacking,' [lawful hacking] consists in the deployment, by investigative authorities, of tools that allow for the intrusion into computer systems, enabling access to its contents."[10]
Metadata	Metadata is "an electronic 'fingerprint' that automatically adds identifying characteristics" to a digital file. These characteristics are not part of the file's viewable content.[11]
Server	A server is a centralized source that manages various computer networks or services.

[7] Cindy Murphy, *What are Forensic Artifacts?-My Favorite Artifacts, Part 0*, Tetra Defense (2020), https://www.tetradefense.com/digital-forensics-services/what-are-forensic-artifacts-my-favorite-artifacts-part-0/.
[8] *Geofencing*, OXFORD LANGUAGES DICTIONARY (3d ed. 2020).
[9] WIKIPEDIA, https://en.wikipedia.org/wiki/IP_address (last visited July 19, 2021).
[10] Carlos Liguori, Exploring Lawful Hacking as a Possible Answer to the 'Going Dark' Debate, 26 Mich. Telecomm. & Tech. L. Rev. 317, 317 (2020).
[11] "What is Metadata?" Harvard Law School, https://hls.harvard.edu/dept/its/what-is-metadata/ (last accessed October 17, 2021).

Introductory Considerations for Prosecutors

1. **Recognize the high probability of encrypted or remotely stored relevant digital evidence in nearly every criminal case.**

Scenario

The cloud-storage company Massiv recently announced that it would, within the next few months, begin to implement encryption for all users and would not store encryption keys. Concerned that this could affect her case by limiting her access to critical evidence, Det. Rhue reaches out to Deputy District Attorney (DDA) Kirstie Savik, who provides legal counsel to the regional Internet Crimes Against Children (ICAC) Task Force and has reviewed Det. Rhue's previous search warrants to electronic service providers. DDA Savik shares Det. Rhue's concern and starts to research exigent circumstances with regard to remotely stored data.

Digital evidence exists in almost every criminal case and provides unparalleled corroborative utility, particularly for crimes usually committed in secret, such as child exploitation. This evidence is increasingly stored remotely on servers across state lines, around the globe, and even orbiting the earth.[12] "Law enforcement officials report a significant increase in the use of known distribution platforms, including 'instant messaging services, peer-to-peer networks, online file-storage services (cloud), anonymous networks, photo-sharing apps, and mobile-only apps' as well as an increase in the use of 'e-mail and photo-sharing websites to distribute'" child sexual abuse material (CSAM).[13] In fact, very little digital evidence remains unconnected to the cloud. Moreover, offenders are going to increasing lengths to hide this evidence and evade apprehension.[14] 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.[15]

[12] 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.
[13] Susan Hennessey, "The Elephant in the Room: Addressing Child Exploitation and Going Dark," Hoover Institution (2017), https://www.lawfareblog.com/elephant-room-addressing-child-exploitation-and-going-dark (last accessed November 5, 2021).
[14] *Id.*
[15] Robert J. Peters et al., Not an Ocean Away, Only a Moment Away: A Prosecutor's Primer for Obtaining Remotely Stored Data, 47 Mitchell Hamline L. Rev. 1073, 1074 (2021).

2. Consider the applicability of existing case law addressing exigent circumstances to remotely stored data.[16]

Scenario

Recognizing both the exigent circumstance and the technical complexities involved—and not wanting to run afoul of any established precedent outside her knowledge—DDA Savik conducts research. She realizes that neither the CLOUD Act nor the bilateral agreement with the country where Massiv is based addresses or defines exigent circumstances. The case law she locates, *U.S. v. Wolfenbarger*, 2019 WL 6716357 (N.D. Cal.. 2019), helps her understand how a service provider's "private search of its own user's account for [its] own independent business reasons" can, without violating the Fourth Amendment, provide the probable cause needed to write an effective search warrant for content within the provider-identified target account.

While obtaining a search warrant prior to conducting a search is always the preferred course of action, it may not be possible to do so in certain pressing situations; exigent circumstances may necessitate a search before a warrant can be obtained. The Supreme Court has decided a handful of warrantless search cases regarding exigent circumstances,[17] though most jurisdictions do not yet have concrete guidance given the minimal appellate challenges and ever-evolving nature of technology and remotely stored data. However, we can apply some key arguments from existing case law to cloud accounts in child exploitation cases.

Courts have consistently held that warrantless searches are permitted when individuals are in danger, such as when searching for violent crime suspects or kidnapping victims, or when there is a high probability that a child is being sexually exploited.[18] Because of courts' demonstrated concern with the safety of minors and protecting them against sex trafficking and exploitation, it is possible

---

[16] "...an ISP [internet service provider] is not a government agent when it searches a user's account pursuant to the ISP's own independent business motivation." *United States v. Wolfenbarger,* 2019 U.S. Dist. LEXIS 213890 at 52 (denying defendant's motion to suppress evidence, despite Yahoo's search of defendant's account for child sexual abuse material).

[17] *See Missouri v. McNeely*, 569 U.S. 141 (2013) (holding that exigency must be determined on a case-by-case basis; natural metabolization of alcohol in the bloodstream does not present a per se exigency exception to search warrant requirement for nonconsensual blood testing in all drunk driving cases); *Riley v. California*, 573 U.S. 373, 391 (2014) (holding that warrantless search of cell phone data was an illegal search and seizure, but noted that if police could demonstrate a *true "now or never" situation* like an imminent remote-wipe attempt, they could rely on exigent circumstances) (emphasis added); *Carpenter v. U.S.*, 138 S.Ct. 2206 (2018) (noting that while the government must generally obtain a search warrant to obtain cell-site location information from a wireless carrier, there are case-specific exceptions that allow for a warrantless search, such as "the exigencies of the situation").

[18] *See, e.g., State v. Buck*, 100 N.E.3d 118, 128-29 (Ohio Ct. App. 2017) (allowing warrantless search of cell phone when "still-missing kidnapping victim's life was in danger, and the police reasonably believed that the phone had been used in the kidnapping operation. The exigency did not evaporate upon the recovery of Buck's cell phone and his arrest."); *United States v. Caraballo*, 831 F.3d 95 (2nd Cir. 2016) (holding that pinging defendant's cell phone to determine his location after woman he had threatened previously was found murdered and he presented an actual immediate threat to others); *United States v. McHenry*, 849 F.3d 699 (8th Cir. 2017) (finding warrantless tracking of defendant's phone was proper when missing child was advertised as an escort in connection with defendant's phone number); *United States v. Gilliam*, 842 F.3d 801 (2nd Cir. 2016) (allowing warrantless tracking of defendant's phone when he abducted his 16-year-old girlfriend and forced her to work as a prostitute); and *State v. Muhammad*, 194 Wash.2d 577 (Wash. 2019) (noting that while cell-site location information was "private affair" protected under Washington constitutional right to privacy, and one-time ping to locate cell phone was intrusive of privacy, exigent circumstances requiring police to act immediately were present in murder investigation).

that these same principles may extend to a warrantless search of remotely stored data that is believed to contain evidence of child exploitation and is at risk of remote wiping.

In *United States v. Flores-Lopez*, the 7th Circuit considered the warrantless search of the defendant's cell phone at the scene of a drug sale and arrest.[19] While the intricacies of technology may make it difficult to determine where to draw the line in an electronic search, searches that are minimally invasive and relevant to the crime for which the individual is arrested are permissible.[20] Further, the 7th Circuit noted that there is always the possibility of remote wiping, a capability possessed by all major cell phone platforms and particularly in larger criminal organizations.[21] Individuals who exploit children often do not act alone—there are vast networks of both CSAM suppliers and consumers—and it would be possible to establish protocols to wipe an individual's remotely stored data upon their arrest. Even acting alone, it is possible for an individual to schedule periodic or triggered wiping of their remote data. Because this remote wiping may include the destruction of relevant evidence in child exploitation cases, and in light of courts' inclination to protect minors from exploitation, it may be possible to use the destruction of evidence exigency to justify a warrantless search of an individual's electronic devices and remotely stored data—though a warrant is clearly preferable and recommended.

3. Understand the limitations, context, and key implications of the Stored Communications Act (SCA).

Scenario

DDA Savik is only marginally comforted by her reading of the *Wolfenbarger* case because the tip regarding K.S.'s identity didn't originate from either the T-Gram or the Massiv service providers. Instead, DDA Savik knows her main concern should be the SCA, since it prohibits electronic service providers from disclosing communications content. Even though the SCA makes a provision for exigent circumstances, and even though plenty of case law exists to support warrantless cellular pinging or tracking in exigent circumstances, obtaining content seems murkier than obtaining a location. Only a single case from a state appellate court covers the search and seizure of a cellular phone's contents in exigent circumstances. While that search was upheld, DDA Savik knows information stored on a mobile device is treated differently from information stored in the cloud, even if the cloud data is accessed from that mobile device.

Prior to 1986, investigators relied on third-party doctrine to justify warrantless searches of personal information from telephone companies and banks. Because customers had voluntarily released this

[19] *United States v. Flores-Lopez*, 670 F.3d 803, 804 (7th Cir. 2012).
[20] *Id.* at 807.
[21] *Id.* at 808.

information, courts held, they relinquished their reasonable expectation of privacy.[22] That changed with the passage of the Electronic Communications Privacy Act (ECPA), which included the Stored Communications Act (SCA). 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."[23] It 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.[24] To that end, the SCA created three categories of data: non-content subscriber data (account holder name and address); non-content transactional data (connectivity to account data); and content data (open and closed emails, group membership).[25] The categories correspond to increasingly stringent levels of legal process.[26]

The SCA originally only gave power to law enforcement agencies in the domestic realm—investigators from one state were able to obtain stored communications on servers in a different state under the long-arm jurisdiction theory.[27] The Act attempted to remedy jurisdictional difficulties by domesticating the legal process.[28] Rather than relying on the individual local laws that typically created an arduous process for out-of-state officers, the Act created a broad jurisdictional nexus.[29] However, Congress enacted the SCA in 1986, long before the development of the technology we have today—before smartphones or global cloud-based data storage.[30]

The SCA's definitions of "electronic storage," in fact, are challenging to apply. "In particular, courts continue to struggle with whether documents stored remotely, such as web-based email, are stored 'for purposes of backup protection' or for some other purpose that would render them outside the scope of the SCA's definition."[31] Moreover, although it's generally understood and accepted that unsent messages stored to a server pending delivery count as "in electronic storage," and messages or other content stored locally to a device do not count the same way, email or other messages stored on a server even after delivery and receipt could be defined either way—and courts are divided on how to count them.[32]

When it comes to exigent circumstances, the SCA allows providers to disclose the contents of a communication, as well as information concerning a subscriber or customer of a service, to "a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications

---

[22] *See Smith v. Maryland*, 442 U.S. 735 (1979); *United States v. Miller*, 425 U.S. 435 (1976). For an in-depth discussion of the third-party doctrine, see Peters et al., *supra*, at 1075-1077.
[23] Peters et al., *supra.* (citing 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))).
[24] *Id.* (citing Rudolph J. Burshnic, Applying the Stored Communications Act to the Civil Discovery of Social Networking Sites, 69 WASH. & LEE L. REV. 1259, 1262 (2012)).
[25] *Id.* at 1077 (citing DAVID W. HAGY, NAT'L INST. OF JUST., DIGITAL EVIDENCE IN THE COURTROOM: A GUIDE FOR LAW ENFORCEMENT AND PROSECUTORS 3 (2007)).
[26] *Id.*
[27] *Id.* at 1079.
[28] *Id.*
[29] *Id.*
[30] *Id.* at 1078.
[31] Michael E. Lackey and Oral Pottinger, "Stored Communications Act: Practical Considerations," Mondaq (2018), available at https://www.mondaq.com/unitedstates/privacy-protection/717180/stored-communications-act-practical-considerations (last accessed October 17, 2021).
[32] *Id.*

relating to the emergency."[33] This allowance applies to providers of either an RCS (Remote Computing Service) or ECS (Electronic Communication Service).

This exception is combined with other legal mandates, including "a court order, warrant, subpoena, statutory authorization, or certification," that make it permissible for electronic service providers to provide information without concern for legal repercussions.[34] Thus, the SCA takes the decision-making burden of whether and how to comply with requests for information off the service or storage provider and instead rests it on courts around the country. As a result, applying the SCA's definitions of both "electronic storage" and "exigent circumstances" is often dependent on the jurisdiction.

4. Understand that case law regarding the decryption of encrypted devices and data continues to evolve.

Scenario

DDA Savik's experience has been that investigators approach cloud service providers when suspects either destroy or refuse to unlock their encrypted smartphone. She knows encryption is still a legal minefield, especially when it comes to whether passwords should be considered testimonial. She's never served legal process on Massiv before, and she doesn't know how responsive they might be to any law enforcement request, much less one based on exigency.

Thus, even though Massiv's implementation of encryption is still a few months off, DDA Savik knows it could take time for them to return information in response to a search warrant. In addition, Massiv didn't provide an exact timeline of implementation, including whether users would be able to test the feature in advance, whether rollout would be staggered, or when rollout would begin. DDA Savik needs to be prepared for the possibility of a true no-win scenario, unless she can find a workaround.

Just because data may be backed up to the cloud doesn't mean the provider can actually access it. The provider may not have access to the encryption key, for one. Data can also be "sharded," or split into chunks, with each chunk encrypted separately.[35]

Even if probable cause exists for a search under the Fourth Amendment, courts are divided on whether compelling a biometric or password decryption key violates the Fifth Amendment right not to self-incriminate.[36] To assert the privilege against self-incrimination, a witness must demonstrate the information sought is compelled, incriminating, *and* testimonial—an explicit or implicit word or act

[33] 18 U.S.C. § 2702(b)-(c).
[34] 18 U.S.C 2703(e).
[35] Timmappa Kamat, "How to Encrypt a Google Doc?" TechTricksWorld, February 1, 2021, available online at https://www.techtricksworld.com/how-to-encrypt-a-google-doc/ (last accessed November 5, 2021).
[36] In the Matter of a White Google Pixel 3 XL Cell Phone, 2019 WL 2082709 (D.Idaho 2019).

that communicates an assertion of fact, which in turn must delve into the contents of one's mind to incriminate.[37]

Courts rely on extensive precedent holding that bodily characteristics are non-testimonial.[38] To search a device without its owner's consent, then, the government can request a search warrant to compel facial, fingerprint, or voice recognition to unlock the device. On the other hand, courts are struggling with the concept that the bodily characteristic can incriminate the owner, by communicating that the person had possession and control of the device and authenticating the device's contents. One such argument is that using compelled biometric data to prove possession and control can provide too much access to the inner workings of a suspect's mind. On the other hand, the act of providing a bodily characteristic has no testimonial significance.[39] Additionally, where bodily characteristics aren't used, or the device owner fails to use their facial, voice, or fingerprint recognition within eight hours, many devices revert to using passcode protection—potentially a shakier Fifth Amendment issue, since a password or passcode exists entirely within a person's mind.

This concern over the compelled use of biometrics may be overcome by demonstrating independent sources or extrinsic evidence for any potentially testimonial aspects of decryption, or through the "foregone conclusion" doctrine. Courts are divided on these strategies. In the 11th Circuit Court of Appeals, the government must show proof of the existence of a password and proof the device contains evidence to allow compelled use of biometrics.[40] The 3rd Circuit agrees on proof of the existence of a password but requires proof that the defendant knows the password.[41] Establishing a foregone conclusion isn't impossible, but it requires leveraging investigative details. It may consist of relying on victim or witness statements, video surveillance footage of a suspect using their device, forensic examinations of password managers, and so on.

State laws may differ, and from a strategic standpoint, not every case might be the "right" case to compel decryption. For all these reasons, in exigent circumstances prosecutors and investigators may ask electronic service providers for emergency access to data in addition to seeking a warrant for the data, bearing in mind that not every provider may cooperate.

---

[37] *Doe v. United States*, 487 U.S. 201, 202 (1988).
[38] Why are bodily characteristics non-testimonial and outside the ambit of the Fifth Amendment? Though providing "real or physical evidence" that may be incriminating, if the act is used to measure physical properties, it is not a communication, but rather the mere exhibition of a physical characteristic. *United States v. Dionisio*, 410 U.S. 1, 7 (1973) (holding that compelled voice exemplars were sought for their tone and manner, not content).
[39] *Doe v. United States*, 487 U.S. 201, 211 (1988).
[40] *In Re Grand Jury Subpoena*, 670 F.3d 238 (11 Cir. 2012)
[41] *U.S. v. Apple Mac Book Computer*, 851 F.3d 238 (3d Cir. 2017).

5. Immediately send letters of preservation for remotely stored data with potential evidentiary value.

Scenario

Regardless of Massiv's potential response, DDA Savik knows her first step is to preserve any evidence associated with the account. A subpoena sent to T-Gram reveals the email address and account information associated with the K.S. username Graciela has been communicating with. DDA Savik uses this information to write preservation letters to both Massiv and T-Gram.

Given the complexity of remotely stored data, law enforcement must immediately send a letter of preservation to relevant internet service providers that can access the desired evidence[42]—not just content but also data such as IP addresses associated with the stored content.[43] Without taking this step, law enforcement risks losing the data to further encryption or complete deletion. 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.[44] Preserving data is a critical tool to prevent destruction or loss of evidence while obtaining additional legal authority.[45] 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, encrypting content, using remote wiping programs or signals, or automated actions of the service provider, such as routine deletion processes.[46] The preservation letter should also contain language prohibiting the service provider from notifying the customer of the legal process.

[42] Peters et al., *supra* at 1105 (citing 18 U.S.C. § 2703(f)(1) (2018)).
[43] Hennessey, *supra.* at 8.
[44] Peters et al., *supra* at 1105 (citing 18 U.S.C. § 2703(f)(1) (2018)).
[45] Peters et al., *supra* at 1105.
[46] Peters et al., *supra* at 1105 ("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]).

6. When in doubt, get a search warrant.

Scenario

DDA Savik's next step is to serve both providers with a 2703(d) order under the SCA to obtain non-content subscriber information, including IP addresses used to upload the content. She will use the IP address to subpoena the service provider who assigned it, in an effort to find the suspect's residential address and—hopefully—Graciela. While she's waiting on this information, Det. Rhue begins to draft her search warrants for the suspect's home, personal mobile device(s), and accounts. The circumstances may be exigent, but she wants to have all her bases covered:

- If the provider returns no information, it may only be possible to access the evidence via the device that uploaded it.
- There's an outside chance that the suspect's device will be unlocked at the time of seizure; for instance, if he's using it as the warrant team comes through the door. In that event, Det. Rhue wants to be able to seize the unlocked device so she can search for locally stored messages, video content, and other relevant evidence, and document additional potential apps or services to serve process on. Searching the device would not only be to corroborate what is on Graciela's device but also to potentially identify other victims.
- However, the suspect's device is just as (if not more) likely to be locked. In either case, DDA Savik counsels Det. Rhue that she cannot access cloud-based data during her search without another search warrant for the data on those accounts. Serving additional, simultaneous search warrants on Massiv and T-Gram for access to the

Sometimes exigency can be avoided with proactive approaches and thorough search warrant drafting. Proactivity of course begins with obtaining search warrants in the first place.

The SCA empowers a court of competent jurisdiction—either a federal or state court, provided the court has jurisdiction over the offense[47]—to issue a subpoena, court order, or a search warrant for the search and seizure of any information delineated in the Act.[48] 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."[49]

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.[50] While the standard is not proof beyond a

[47] *Id.*
[48] Peters et al., *supra* note 2, at 1079 (citing 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 at § 2703(d) (2019)).
[49] *Id.* (citing 18 U.S.C. § 2711(3)(B) (2018) (emphasis added)).
[50] Peters et al., *supra* at 1102.

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.[51] The items to be searched must be equally sufficiently described to avoid the government from unfettered searches of a location not otherwise relevant to the crime under investigation.[52] 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.[53]

The prudent professional will acquire at least two search warrants when encountering remotely stored data. First, the investigator should seek a search warrant for the relevant physical device(s). Second, the investigator should follow up with search warrants to each relevant cloud account provider connected to the device.

7. Anticipate the particularity requirement when drafting search warrants and warrant templates for remotely stored data.

Scenario

Graciela's screenshots are time- and date-stamped to the extent that Det. Rhue has a good general sense of when Graciela started to talk to the suspect. DDA Savik counsels her to narrow her search warrant to this time frame. She offers Det. Rhue a template that demonstrates how she can search the device thoroughly, beyond just the T-Gram and Massiv accounts, but still on a limited basis.

Det. Rhue argues that there could be other victims, and she wants to be able to extend the search out longer. However, DDA Savik is opposed, since she has no reason to believe that other victims exist, outside of academic literature indicating the high number of average victims per offender. However, if during the narrow search Det. Rhue does find evidence of other victims, she can then obtain one or more additional search warrants to add to her case.

The Fourth Amendment requires that a search warrant articulate facts to establish probable cause and also particularly describe the place to be searched and the persons or things to be seized.[54] The particularity requirement guards against general searches that allow officers executing the search warrant unguarded discretion regarding what items may be seized.[55] Cloud data requires the same articulation—the probable location of the data (the user account) and clear facts showing the likelihood of the requested data being in the location to be searched.

---

[51] Peters et al., *supra* at 1102 (citing *Illinois v. Gates*, 462 U.S. 213, 214 (1983)).
[52] Peters et al., *supra* at 1102 (citing United States v. Riley, 906 F.2d 841, 845 (2d Cir. 1990)).
[53] *Id.*
[54] U.S. CONST. Amend. IV.; Groh v. Ramirez, 540 U.S. 551, 557 (2004).
[55] *United States v. Riley,* 906 F.2d 841, 844 (2d Cir. 1990).

Compiling sufficient and necessary facts to describe the location of the data and the likelihood of the data being in that location requires basic police work. Connecting user names, associate email addresses, IP addresses, and subscriber information supports the claim that the search warrant is targeting the appropriate service provider and account. In cases of child exploitation, a forensic interview can yield important facts and information regarding the location of cloud data. A forensic interview should obtain, in a developmentally appropriate manner, as many details as possible from the child, including details of the technology used during the exploitation.[56]

Particularly describing what and where to search within the scope of the Fourth Amendment also means limiting the time frame of your search to a period that has a nexus to probable cause. While investigators may be interested in reviewing all available data related to a particular user, only data from certain time periods may be relevant. A detailed explanation of why that time frame will likely include relevant evidence may increase the chances of being issued the search warrant.[57] Investigators can apply for a fresh search warrant if additional evidence arises that suggests the search should be expanded to other time frames.

Search warrant affiants should be prepared to articulate a concrete description of the data requested. However, courts grant latitude to officers in determining relevant data. The *Riley* court evaluated this issue with a search warrant seeking evidence of drug activity and acknowledged "allowing some latitude in this regard simply recognizes the reality that few people keep documents of their criminal transactions in a folder marked 'drug records.'"[58]

Officers searching for evidence in child exploitation cases will face similar barriers while combing through potential sources of digital data. It is well established that offenders in child exploitation investigations who have a sexual interest in children are likely to possess and collect child sexual abuse material (CSAM),[59] to which both the internet and digital cameras have increased access. For preferential-type sexual offenders, collection is the key word: they do not merely view CSAM; they save it. It comes to define, fuel, and validate their sexual fantasies.[60]

Some courts have recognized that officers may first obtain all relevant data from a service provider and then inspect it to determine whether the data is responsive to the warrant.[61] This procedural approach allows law enforcement to seize and search data relevant to the investigation and make reasonable determinations as to its evidentiary value.[62] For child exploitation cases this technique may be helpful, in that it does not limit officers to narrow search methods like a "keyword search,"

---

[56] Victor I. Vieth, When the Child Has Spoken: Corroborating the Forensic Interview, 2(5) CENTERPIECE 1 (2010).
[57] *United States v. Blakstad,* 2020 U.S. Dist. LEXIS 188133.
[58] *Riley,* 906 F.2d at 845.
[59] Kenneth V. Lanning. *Child Molesters: A Behavioral Analysis (5th Ed.).* Alexandria, VA:, National Center for Missing and Exploited Children (2010).
[60] *Id.*
[61] *United States v. Blakstad,* 2020 U.S. Dist. at 24 (finding a warrant limiting the search of email messages to a period of approximately 15 months before the first allegedly unlawful transaction was a reasonable restriction given the evidence provided.)
[62] *See In re* A Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@Gmail.com Maintained at Premises Controlled by Google, Inc., 33 F.Supp. 386 (2014) and *United States v. Bowen,* 689 F.Supp. 675(2010) for further discussion on police searches of extensive digital data.

given the reality that child predators (like drug dealers) do not typically keep their contraband in clearly marked folders advertising their illicit contents.

Probable cause exists if, under the totality of the circumstances, there is fair probability that contraband or evidence of a crime will be found at a specified location. All that is required is the information in the affidavit not be stale.[63] In *Adams v. State*, the court rejected the defendant's argument of staleness because only three months had elapsed between the discovery of CSAM and the execution of the search warrant.[64] The *Adams* court reasoned that the nature of CSAM images allowed investigators to make a reasonable assumption that the material was saved or recoverable despite the time lapse due to the "hoarding" nature of sexual offenders.[65] In *United States v. Vosburgh*, the court also rejected a staleness argument, since "as we have long recognized, persons with an interest in child pornography tend to hoard their materials and retain them for a long time."[66] "Child pornography is illegal, and therefore difficult and risky to obtain. Presumably, once a child pornography collector gets his hands on such material he will not be quick to discard it."[67] Some courts have rendered defense-oriented rulings where prosecutors were unable to articulate a reason for lengthy delays, but most courts currently follow *Vosburgh*'s approach.

8. Mitigate the impact of investigative techniques on uninvolved citizens.

Scenario

Graciela did not screenshot any messages telling her to meet at a particular location, but Det. Rhue has found a location search for a convenience store about two blocks away from Graciela's school. The convenience store has CCTV cameras, and Det. Rhue asks for footage from the date of Graciela's disappearance. DDA Savik wants a geofence search warrant to see if a number matching K.S.'s T-Gram subscriber information is present. She knows the relevant time period will still net convenience store customers, so she again advises Det. Rhue to narrow the time range only to the timestamps on the footage from that day, taking care to ensure the CCTV's time stamps were properly calibrated and recorded.

Sometimes, investigative techniques involve a high probability of collecting the data of uninvolved citizens. For example, law enforcement may employ devices that mimic cellular towers or obtain evidence directly from a search engine provider. If these techniques are used, it is critical for prosecutors and law enforcement to proactively address privacy concerns, and explain how the

[63] *Adams v. State,* 316 So.3d 260, 267 (Ala. Crim. App. Feb. 7, 2020).
[64] *Id.* at 270.
[65] *Id.*
[66] *United States v. Vosburgh*, 602 F.3d 512, 528 (3d Cir. Pa. 2010).
[67] *Id.*

government anticipated, mitigated, and addressed these concerns throughout the investigative process.

Conclusion

As data and the internet generally become more complex, prosecutors and investigators are encountering new challenges with cloud accounts and encrypted data. Exigency is compounded by suspects' use of encryption to protect hard drives, cell phones, and data stored within apps. Hailed as a way to secure consumers against data breaches and government overreach, encryption can also stymie legitimate government efforts to apprehend criminals. To complicate matters, courts are divided on how to handle it. Investigators must understand the interplay of technology and legal process; only then can they plan out next steps at each stage of the investigation to move quickly and effectively, securing evidence and saving lives.

A deeper explanation of this process, along with more advanced discussions on encryption and the use of novel strategies and tools to bypass it, optimal approaches to working with service providers and educating triers of fact, and other legal issues can be found in "Exigency and Encrypted Cloud Accounts, Part 2: 7 Advanced Strategies for Prosecutors."

 This project was supported by Award No. 2019-CI-FX-K006 awarded by the Office of Juvenile Justice and Delinquency, Office of Justice Programs, Department of Justice.