a program of zero abuse PROJECT

Exigency and Encrypted Cloud Accounts (Part 2)

TiPP

7 Advanced Strategies for Prosecutors

By Robert J. Peters, Christa Miller, Joseph D. Remy, & Kathleen Nolan

Encryption and remotely stored data have become ubiquitous in criminal investigations, yet the Stored Communications Act 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 offered eight introductory considerations for prosecutors dealing with exigency and encrypted cloud accounts,[1] while Part 2 addresses more advanced strategies for dealing with cloud providers and other stakeholders.

Specifically, Part 1 examined how technology providers increasingly are encrypting both data and devices to preserve user privacy. Previously, the use of encryption was standard operating procedure only for sensitive or classified material, such as military intelligence, intellectual property, and banking or other financial information. But now, encryption methods proliferate. Consumer phone and computer developers have begun to introduce standard features—Secure Enclave in Apple devices, for one, or the full disk encryption shipped with later versions of the Android operating system—that protect users' stored data ("data at rest"). Users can also install so-called "vault" apps to encrypt the data themselves. App developers are deploying encryption to protect data transmitted over the internet as well ("data in motion"): "End to end encryption" is a notable feature of mobile messaging apps like Signal, Telegram, and WhatsApp, where messages are encrypted by the sender and decrypted by the recipient all within the app.

This increase in encrypted data has slowed and sometimes stymied criminal investigations. However, a number of methods can be used to break encryption when a device owner has refused, or is unavailable, to provide access. Gaining access may be as simple as finding the passcode written down inside their desk or guessing an easy-to-remember code such as their birthday—though this method has its risks. More complex methods include the use of "brute force" attacks via hacking tools. The company Grayshift made waves when it introduced its GrayKey tool, which exploits vulnerabilities in Apple iOS software to crack encryption.[2]

---

[1] Robert J. Peters, Christa Miller, Kathleen Nolan, Caralea Grant, & Lauren Munday, "Exigency and Encrypted Cloud Accounts, Part 1: 8 Introductory Considerations for Prosecutors," ZERO ABUSE PROJECT, 2022.
[2] Thomas Reed, "GrayKey iPhone unlocker poses serious security concerns," MALWAREBYTES LABS, March 15, 2018, available at https://blog.malwarebytes.com/security-world/2018/03/graykey-iphone-unlocker-poses-serious-security-concerns/ (last accessed November 5, 2021).

Because forcing decryption can introduce Fifth as well as Fourth Amendment implications, using any of these methods in exigent circumstances depends on the severity of the crime, the type of encryption, the method itself, and the complexity of the code. For example, a four- to six-character passcode may take only hours to crack, but a 12-character pin would take centuries. Moreover, few law enforcement agencies have the time or resources to deploy many of these methods, even in exigent circumstances.

As a workaround, many law enforcement investigators began to "bypass" encrypted devices by approaching cloud-based service providers for the data instead. However, the concurrent global debate around privacy has led many providers to roll out encryption on those platforms as well. Facebook is the most notable of these, announcing in 2019 its plans to expand end-to-end encryption from WhatsApp to its Messenger platform.[3] As a result, just because data may be stored in the cloud doesn't mean the provider can actually access it, especially if the provider doesn't retain access to the encryption key.[4]

With yet another avenue to data access quickly disappearing, how can prosecutors best preserve and procure vital evidence in child exploitation cases? Below are seven strategies for strengthening your data collection efforts—from persuading judges and service providers to exploring novel strategies and technologies, to analyzing successes in other countries.

Advanced Strategies for Prosecutors

1. Educate triers of fact on complex technologies and legal doctrines with accessible language.

Scenario

The judge assigned to evaluate search warrants in the Graciela Montoya missing child case is newly appointed, and Deputy District Attorney (DDA) Kirstie Savik has never worked with her before—nor has she ever approached a judge with a geofence search warrant. After carefully studying emerging case law on geofence warrants, she solicits help from another prosecutor in a neighboring jurisdiction, DDA J.T. Kirk, who has a reputation for not believing in no-win scenarios and, perhaps as a result, has successfully had geofence search warrants approved. DDA Kirk helps DDA Savik to explain: (1) why encryption (in addition to the case circumstances) renders the circumstances exigent, (2) the foundations of how encryption and geofences work, (3) the other investigative steps that have been taken to find both the suspect and Graciela, and (4) how a geofence search would help.

[3] Mark Zuckerberg, "A Privacy-Focused Vision for Social Networking," FACEBOOK, March 12, 2019, available at https://www.facebook.com/notes/2420600258234172/ (last accessed September 26, 2021).
[4] Tomaso Vasella, "Data Encryption in the Cloud: BYOK, BYOE, HYOK and Tokenization," SCIP AG, November 5, 2020, available at https://www.scip.ch/en/?labs.20201105 (last accessed September 26, 2021).

Judges often push back on signing a search warrant for data when they don't understand how the technology works or the data's relevance to an investigation. The difficulty of articulating exigency, particularity, foregone conclusions, and other elements for a search—much less how the technology impacts an individual's privacy and the reasonable expectation thereof—is compounded by the fact that technology is often a black box, its operations concealed behind developers' nondisclosure agreements. Few attorneys understand the technology well enough to clearly state their request, its relevance, and its reasonableness so that judges and jurors can make informed decisions.

Organizations like the U.S. Secret Service's National Computer Forensics Institute (NCFI) have tackled these challenges by developing a curriculum for judges.[5] However, the burden of explaining technology as it relates to any given case still falls to prosecutors. On a practical level, prosecutors need to be able to:

- Rely on investigator experts to demystify—without under- or over-explaining—a piece of technology to a judge responsible for signing a search warrant.
- Pay meticulous attention to the particularity requirement, including showing how a search warrant minimizes the scope of intrusion and enables the finding of exculpatory *Brady* material.

Such explanations become more pressing in exigent circumstances, so the time to prepare an expert or to call on them for assistance is not during an emergency. Instead, prosecutors are advised to build relationships with experts both during and outside the context of an investigation. What an investigator knows and how they communicate it can be crucial to securing a judge's approval for a search—and, ultimately, a jury's fair assessment of the evidence.

Where We Left Off

The following case scenario, detailed in Part 1 and summarized below, highlights common issues that arise with digital evidence in suspected child exploitation cases. It continues throughout Part 2.

Deputy District Attorney (DDA) Kirstie Savik is working to locate Graciela Montoya, a minor who's gone missing. There's reason to believe Graciela is being held against her will, and DDA Savik has recently tracked down a phone number associated with a potential captor. Time- and date-stamped messages lead her to believe Graciela made contact with this person—K.S.—at a nearby convenience store right before she disappeared. DDA Savik would like to use CCTV footage from the store paired with a geofence search to fully identify K.S.

[5] "Digital Evidence for Judges (DEJ)," NATIONAL COMPUTER FORENSICS INSTITUTE (NCFI), available at https://www.iacpcybercenter.org/training_conferences/digital-evidence-judges-dej/ (last accessed October 18, 2021).

2. Proactively safeguard innocent subscriber data.

Scenario

With DDA Kirk's help, DDA Savik has successfully convinced the judge that she and the assigned detective, Marla Rhue, are only interested in a single phone number from the geofence. DDA Savik's strategy of narrowing the geofence time frame to only the relevant date and time stamps on the CCTV cameras worked; she was able to show that the search would not expose any other numbers' protected movements after their owners departed the convenience store during that specific time frame. In addition, her assurance that she'll seek a second warrant to fully identify the owner of the device associated with the phone number helped to win over the judge.

Much of the media concern around "reverse" warrants for geofence or search data—or the use of cellular tower dumps or, for that matter, a device designed to mimic a cellular tower—is about the prospect of a "digital dragnet." In attempting to identify a single suspect, the State might also sweep up the data of uninvolved citizens going about their daily business.[6] The concern isn't completely unfounded; take, for instance, the 2018 wrongful arrest of Jorge Molina, whose Google location data ostensibly placed him at the scene of a murder. However, the data had already been shown to be unreliable.[7]

In exigent circumstances, when time is of the essence, such mistakes are an even greater risk, and prosecutors and investigators should show they've mitigated any hint of tunnel vision or similar biases; a judge will weigh the exigency against the intrusiveness. The use of search warrants, even in exigent circumstances, is strongly recommended. With reverse warrants in particular, part of educating a judge is showing how a two- or three-step process relies on anonymized device data from one or more very narrow time periods. By using context to reduce the possibility of false positives, prosecutors can establish the probable cause to seek a fresh search warrant for the account-owner information associated with a specific device,[8] thereby demonstrating sensitivity to subscriber information.

[6] Zack Whittaker, "Google says geofence warrants make up one-quarter of all US demands," TECHCRUNCH, August 19, 2021, available at https://techcrunch.com/2021/08/19/google-geofence-warrants/ (last accessed September 26, 2021).
[7] Meg O'Connor, "Avondale Man Sues After Google Data Leads to Wrongful Arrest for Murder," PHOENIX NEW TIMES, January 16, 2020, available at https://www.phoenixnewtimes.com/news/google-geofence-location-data-avondale-wrongful-arrest-molina-gaeta-11426374 (last accessed September 26, 2021).
[8] Christa Miller, Katherine Hansen, & Joseph Remy, "The Third Party Doctrine Is Under Scrutiny. Will It Hold Up?" MEDIUM, February 24, 2021, available at https://medium.com/forensic-horizons/the-third-party-doctrine-is-under-scrutiny-will-it-hold-up-d3830c8ccf03 (last accessed July 16, 2021).

3. Consider optimal approaches to working with service providers, especially when it comes to Stored Communications Act limitations.

Scenario

The messaging app T-Gram has responded to the 2703(d) order sought by DDA Savik (in Part 1) with an IP address, which Det. Rhue traces to a server in Ukraine. That's bad luck: she believes the suspect is using a VPN to mask his location. Still, given the exigency, DDA Savik thinks if she approaches the cloud service Massiv (where K.S. claimed to store videos he was using to blackmail Graciela) with the IP address alone, she may be able to get them at least to preserve any content uploaded to their servers from that IP address, even if they can't capture the full extent of the suspect's activity.

Meanwhile, the cellular provider identified in the geofence search says the phone number from the geofence is associated with a "burner" SIM card, so they cannot provide customer information such as a name or address. However, they do have a record of the SIM card's purchase and activation, and they're able to provide the credit card number used in the transaction. DDA Savik subpoenas the bank that issued the card, providing Det. Rhue with the name and address of the credit card holder.

Provider pushback against court orders, including search warrants, has been extensively covered in news media. Nonetheless, a proactive approach to working with service providers—through both provider partnerships and technical solutions—can help streamline processes and communication long before exigency arises.

First, prosecutors should know what data they're asking for, why it's needed for a case, and the legal grounds for getting it. The more intrusive the search, the more stringent the legal process; for instance, obtaining non-content subscriber information and metadata requires a lower burden of proof than obtaining content or real-time location information.[9] As previously discussed in Part 1, attention to the Fourth Amendment's particularity requirement improves a search warrant's chances of being signed, as well as the likelihood that an argument for exigency will be upheld if challenged or appealed.[10]

By the same token, use of boilerplate search warrant templates can do the opposite of what they intend. If the language is inaccurate, incomplete, or otherwise doesn't match what a provider offers—which could change depending on how the provider delivers its services—that lends credence to a provider's argument that the warrant is "overbroad." Instead, warrant templates should be provider-

[9] Joseph Remy, Katherine Hansen, Abigail Abraham, Robert Peters & Christa Miller, "Judge, Jury… Service Provider? 6 Strategies for Prosecutors Confronting Objections from Electronic Service Providers," ZERO ABUSE PROJECT (2022).
[10] Peters et al., *supra*.

specific and regularly reviewed and updated, and warrant affidavits should be carefully examined to be sure they contain case-specific facts that support probable cause.[11]

Communication can help prosecutors build trust with providers' law enforcement liaisons so that when there's a delay, the prosecutor has a better sense for the rationale. Many times, a delay could be the result of a provider's overworked or under-resourced staff. Prosecutors should assume good faith but, in exigent circumstances, may need to take more drastic measures such as a Motion to Compel or Order to Show Cause.[12] In addition, a search warrant should include language that requires the provider to notify the requester if they don't include certain responsive records, and all returns should be validated to ensure the requested data is there.[13] Finally, while the Stored Communications Act allows providers to be reimbursed by the government for the costs associated with data processing, providers cannot withhold records pending payment.[14]

Technical workarounds are another critical avenue for prosecutors and investigators to consider. One novel solution is to obtain cloud-storage service provider consent to access user folders through mechanisms supported by their own interfaces. For example, several providers, such as Google, Dropbox, and Mega, make it possible for users to share content via web URLs or links. With probable cause to believe the links and their associated account contain information relevant to the specified crimes under investigation, and a search warrant in hand reflecting that belief, investigators should be able to lawfully access the links with careful documentation—via screenshots or similar method—of what was accessed and when.[15] Managing the search this way protects investigators from claims that they accessed the storage without legal authority, which is prohibited under 18 U.S.C. 2701, *et seq.* Instead, they can rely on judicial sanction (via search warrant) to conduct the search, facilitated by the service provider in real-time.

In a similar vein, it may be possible to subpoena a service provider for the email address(es) associated with the accounts under investigation, then draft search warrants to obtain communications content from the email provider instead. This strategy could be particularly useful when dealing with service providers outside the country.[16]

---

[11] Remy et al., *supra*.
[12] *Id.*
[13] *Id.*
[14] *Id.*For more information on navigating challenges with service providers, see Joseph Remy, Katherine Hansen, Abigail Abraham, Robert Peters & Christa Miller, "Judge, Jury… Service Provider? 6 Strategies for Prosecutors Confronting Objections from Electronic Service Providers," ZERO ABUSE PROJECT (2022).
[15] *Id.*
[16] *Id.*

4. **Explore novel strategies and technologies to counter child exploiters' escalating sophistication.**

Scenario

Det. Rhue serves the search warrant on the suspect's home. In addition to rescuing Graciela and arresting the suspect, K.S. Noonien, Det. Rhue seizes his devices: a laptop and two mobile phones, one of which doesn't have any standard cellular company logos. All are encrypted, and Noonien refuses to provide either his biometric access or his passcode.

However, a tablet set up in a bedroom for filming is unlocked, and its home screen is in plain view. Multiple apps are displayed, including Massiv. Det. Rhue is tempted to look at the Massiv app for the email address Noonien is using, but DDA Savik reminds her that if she searches the tablet now, she could be in violation of the SCA for accessing cloud-based evidence from the device: only the home screen, not the data behind it, can be considered in "plain view" for the purposes of an exception to the Fourth Amendment. She advises Det. Rhue to photograph the screen before placing the tablet in airplane mode to prevent any potential destruction of evidence. She also advises Det. Rhue to seize the tablet and its charger so she can take it into evidence without powering it down. As soon as she receives Det. Rhue's screenshot, DDA Savik will serve the cloud providers of these apps with preservation letters in advance of the search warrants that Det. Rhue has already prepared. She'll also use the circumstances of seizure to argue probable cause to search the apps for more evidence.

Det. Rhue has also carefully photographed the other devices she is seizing, and she sends DDA Savik an image of the unidentifiable phone to see if she's aware of anything similar in ICAC circles. DDA Savik recognizes it right away: similar devices have been seized in other recent cases, and federal agents on the task force believe it's related to an organized network of human traffickers who are using the "dark" devices to communicate with each other. While she refers Det. Rhue to lab resources that may be able to "crack" the phone and the laptop, DDA Savik learns from the agents that they may never be able to find out what's on the dark device.

Technical workarounds are useful not just with search warrants but also with the technology itself. Take, for example, the network investigative technique (NIT—malware code employed by investigators) used to identify computer users who were logging in to a website known as Playpen. Playpen was an anonymized website housing child sexual abuse material (CSAM), accessible through The Onion Router (TOR) browser.[17]

[17] Orin Kerr, "Government 'Hacking' and the Playpen Search Warrant," WASHINGTON POST (Sept. 27, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/09/27/government-hacking-and-the-playpen-search-warrant/.

TOR sites can only be accessed by logged-in users who know the randomized string of letters and numbers of the website's address.[18] By 2014 when the U.S. government began investigating Playpen, the website had already grown to hundreds of thousands of users. This volume posed a difficult hurdle for investigators: TOR's anonymity included hiding users' IP addresses, making them virtually untraceable. To uncover that many identities, the government obtained two warrants. The first warrant gave them access to Playpen—which they then seized and relocated to a government-controlled server—and the second warrant, known as the NIT warrant, allowed the government to install the NIT on the computers of logged-in users to gain access to their true IP addresses.[19]

Following the Playpen investigation, various courts around the country encountered cases in which defendants challenged the constitutionality of the NIT warrants, with specific claims that the warrants violated defendants' Fourth Amendment rights. These cases displayed how courts can be flexible in their response to new investigative methods in new contexts. They involved grappling with complex, technological searches across various geographical locations and areas of the internet. Although the Playpen case may not exactly mirror issues that arise in encrypted or remotely stored data cases, the cases and decisions stemming from it allow us to better understand the reasoning a judge may use to excuse search warrants whose context raises Fourth Amendment challenges.

Arguably, "the Playpen warrant demonstrates not only how constitutional requirements can be met for so-called watering-hole attacks but also how such warrants can be executed in a manner that is exceptionally strong with regards to constitutional sufficiency."[20] By allowing individuals to have completed an offense by logging into and accessing a website clearly advertising its contraband—in contrast to, say, accessing a site advertising illicit drugs without actually purchasing the drugs—the NIT warrant satisfied both probable-cause and particularity requirements and paved the way for similar policy.[21]

Take, for example, when police in Europe stunned much of the rest of the world in the summer of 2020, after it was revealed that they had used malware in much the same way as the FBI's NIT: to "hack" an encrypted messaging platform used by multiple figures allegedly involved in European organized crime.[22] As in the FBI's Playpen operation, hundreds of suspects were arrested as a result of the EncroChat operation. Although many pleaded guilty, others challenged the legality of this methodology under the law in their own countries, including the United Kingdom, the Netherlands, and Germany.[23] Among the arguments were chain of custody, a lack of information needed to verify the data, the validity of the Targeted Equipment Interference (TEI) warrant that allowed the UK's National Crime Agency (NCA) to search the EncroChat data, and whether the evidence had been intercepted rather than collected—and thus counted only as intelligence rather than evidence.[24] In

---

[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] Joseph Cox, "Encrochat Hack That Brought Down Hundreds of Criminals Faces Legal Challenges," VICE, October 20, 2020, available at https://www.vice.com/en/article/7k9z7x/encrochat-hack-illegal-defense-nca (last accessed September 25, 2021).
[23] Bill Goodwin, "Berlin court reverses ban on use of EncroChat evidence in criminal trials," COMPUTER WEEKLY, September 3, 2021, available at https://www.computerweekly.com/news/252506233/Berlin-court-reverses-ban-on-use-of-EncroChat-evidence-in-criminal-trials (last accessed September 26, 2021).
[24] Cox, *supra*.

addition, the "mass hack" had swept up at least some EncroChat users who were not alleged to have been involved in any illegal activity.[25]

Objections to "mass hacking" (like in the Playpen and EncroChat operations) that emphasize the quantity of individuals caught in the dragnet "[miss] critical operational realities and [misconstrue] the constitutional requirements."[26] Exigency is one such reality. Creative solutions are invaluable when time is of the essence in rescuing children and preserving critical evidence—NITs, mobile-device reverse engineering, emerging methods like side channel analysis and fault injection,[27] legal remedies like the use of wiretapping laws on social media communications,[28] and yet-undiscovered methods all play a part.

Unlike more time-tested digital forensic methods and tools, some of these new methods may not have achieved the general acceptance in the digital forensic community needed to meet admissibility requirements. When forensic examiners use them to bypass encryption, prosecutors should expect a motion to suppress. However, programming vulnerabilities in general are known to have short windows of usefulness between the time a so-called "zero-day" (never-before-seen) exploit can be researched and the time it's patched.[29] In exigent circumstances, where users need to be identified in order to rescue child victims, the use of untested tools or techniques can be argued and defended in good faith.

5. Recognize that technological advances do not inherently give defendants an increased expectation of privacy.

Scenario

Noonien lawyers up and his defense attorney argues that the presence of encryption and the use of the VPN enhance his expectation of privacy. The judge almost agrees until DDA Savik argues otherwise, referring extensively to just such a case decided in federal court.

One defendant in the Playpen case, Michael Lough, argued that by using the TOR browser to hide his IP address and therefore his identity, he had an increased expectation of privacy that voided the government's search warrants.[30] The court disagreed, holding that Lough "voluntarily turned over his

[25] *Id.*
[26] *Id.*
[27] Aya Fukami, Radina Stoykova, & Zeno Geradts, "A new model for forensic data extraction from encrypted mobile devices," FORENSIC SCIENCE INTERNATIONAL: DIGITAL INVESTIGATION, Vol. 38, September 2021, available at https://doi.org/10.1016/j.fsidi.2021.301169 (last accessed August 24, 2021).
[28] Justin Fenton, "Wiretaps for Facebook? Maryland authorities are getting permission to tap digital and social media apps," BALTIMORE SUN, August 9, 2021, available at https://www.baltimoresun.com/news/crime/bs-md-cr-facebook-wiretap-20210809-ulpifhvowrdrvnivqq75j5floi-story.html (last accessed September 26, 2021).
[29] Ohio State University, "What Is a Zero-Day Exploit?" available at https://cybersecurity.osu.edu/cybersecurity-you/avoid-threats/what-zero-day-exploit (last accessed September 25, 2021).
[30] *United States v. Lough*, 203 F. Supp. 3d 747 (N.D.W. Va. 2016)

IP address to every computer with which he made contact, including the first node of the TOR network…. At the very least, Lough certainly knew that he was revealing his IP address to one unknown third party who, for all he knew, was a law enforcement officer."[31]

Even assuming that Lough did have a subjective expectation of privacy, it is not one that society is prepared to recognize as reasonable.[32] Courts have repeatedly held that there is no objectively reasonable expectation of privacy in one's IP address,[33] and moreover, that when government agents obtain IP address information directly from a defendant's computer, "the partially public nature of the IP address is not relevant… the relevant fact is 'how the government obtained the information, not whether it could have obtained the information some other way that would not be a search.'"[34] It should be noted that at least one judge threw out Playpen evidence on jurisdictional grounds,[35] though the vast majority of Playpen cases were upheld on appeal.

Prosecutors could cross-apply language from cases like *Lough* to the context of encryption; usage of complex technology alone is not dispositive of Fourth Amendment issues.

6. Articulate the applicability of the good faith exception to the exclusionary rule.

Scenario

DDA Savik receives a panicked phone call from Det. Rhue. During a personal day she took from work, Massiv responded to DDA Savik's preservation letter by providing the full extent of the content Noonien uploaded—not just the videos he was using to "sextort" Graciela, but everything from the specified time frame, including videos of other girls. Another detective, not realizing that the data was not responsive to a search warrant, looked at the information without consulting Det. Rhue. While the messages confirm that Noonien was indeed grooming other girls, Det. Rhue is anxious that a court will throw out all the evidence because of the other detective's actions.

Because Det. Rhue already served the search warrant on Massiv, even though the warrant and the responsive information "crossed" in transit, DDA Savik reminds her that they had probable cause to search the account for Graciela's videos, and advises her simply to write a second warrant for the other data—and not to look at it again until Massiv responds.

---

[31] *Id.*
[32] *United States v. Castellanos,* 716 F.3d 828, 832 (2013).
[33] *United States. v. Bynum,* 604 F.3d 161, 164 (4th Cir. 2010) (quoting *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) (collecting cases)).
[34] Hennessey, *supra*.
[35] Joseph Cox, "In a First, Judge Throws Out Evidence Obtained from FBI Malware," VICE, April 20, 2016, available at https://www.vice.com/en/article/gv5yqj/in-a-first-judge-throws-out-evidence-obtained-from-fbi-malware (last accessed September 25, 2021).

As Part 1 described, the Stored Communications Act is complex and in some ways outdated. At times, despite law enforcement's best efforts to comply, applying the SCA to a "gray area" may result in greater judicial scrutiny. For example, a provider might go above and beyond a government request by delivering more information than was requested.[36]

Based on the Fourth Amendment, the exclusionary rule holds that evidence obtained through a warrantless search is inadmissible in criminal proceedings.[37] However, the good faith exception allows evidence to be admitted if officers had obtained the evidence in a good-faith reliance on a search warrant that was later found to be defective in some way,[38] or if "the information would have been inevitably discovered by lawful means and/or through an independent source."[39]

This was the case in *United States v. Bowers*, 2021 WL 2882439 (W.D. Pa. 2021), in which Gab, a social media provider, responded to a government preservation letter by voluntarily providing all the data the government had asked them to preserve. The government, "in an abundance of caution," sought a search warrant anyway to show that it had probable cause to search the provided data, which it further stressed had already been publicized by news media. The warrant, having met the particularity requirement, was signed by a magistrate judge. The defendant's motion to suppress didn't argue that the warrant was defective; rather, he moved to suppress the evidence based on the government's warrantless seizure of the non-public data, to which the defendant had a reasonable expectation of privacy. The court disagreed, pointing to the language in the government's preservation letter to support its statement, saying: "[T]here is no evidence that the Government acted to have Gab reveal or in any way provide the information." Further, even if the government had violated the Fourth Amendment, a magistrate judge had reviewed and signed the search warrant after the fact.[40]

A number of federal courts have considered what evidence falls within the scope of a good faith exception, and have developed some consistency regarding the rule. For example, courts have repeatedly allowed the admission of evidence obtained in cases where either electronic service providers volunteered more information than required by a warrant or officers made appropriate inferences regarding the location of evidence.[41] As noted in *Bowers*, exclusion is a last resort, and the goal is to deter Fourth Amendment violations rather than suppress evidence. When officers act in good faith, suppressing evidence creates no deterrent effect.[42]

---

[36] *See, e.g., United States v. Bowers*, 2021 WL 2882439 (W.D. Pa. 2021) (noting that while there was probable cause to connect the defendant to one email account and not others, it was not improper for the government to request and receive access to the other email accounts, and even so, there was no reason for officers to believe that receiving information from the additional emails was illegal).
[37] *Weeks v. United States*, 232 U.S. 383 (1914) at 383.
[38] *United States v. Leon*, 468 U.S. 897 (1983) at 898.
[39] Bowers, *supra.*
[40] Bowers, *supra.*
[41] *See, e.g., United States v. Ackerman*, 804 Fed. Appx. 900 (10th Cir. 2020) (National Center for Missing and Exploited Children's (NCMEC) search of defendant's email fell within good-faith exception to exclusionary rule); *United States v. Flanders*, 468 F.3d 269 (5th Cir. 2008) (holding good-faith exception to the exclusionary rule applied to search of defendant's computer after police officer inferred that persons who abuse children also often collect and possess child pornography); *United States v. Coyne*, 387 F.Supp.3d 387 (D. Vermont 2018) (holding that government agent's review of CSAM image flagged and viewed by electronic service providers (ESPs) fell within scope of private search exception to warrant requirement).
[42] *Bowers*, 2021 WL 2882439 at *5 (citing *United States v. Werdene*, 883 F.3d 204, 215 (3rd Cir. 2018); *Leon*, 468 U.S. at 907; *United States v. Katzin*, 769 F.3d 163, 171 (3rd Cir. 2013)).

Despite jurisdictional differences, certain commonalities arose from judicial rulings in Playpen cases. Although much dicta mentioned that the warrants may have violated the Fourth Amendment, almost all were excused based on the "good faith" of investigators.[43] Additionally, judges were more likely to support the use of the NIT warrant when investigators provided detailed reasoning as to why the warrant was necessary in their affidavits.[44] Certain judges also found the nature of the technology to have implications for "probable cause" for purposes of the search warrant.[45] Additional cases around the United States further echo these findings.[46]

7. Apply strategies and lessons learned in international contexts.

Scenario

In addition to Massiv, Noonien has been using another encrypted cloud storage account. However, although that provider does store the decryption key, it is located in another country that doesn't have a bilateral treaty allowing it to cooperate with U.S. CLOUD Act provisions. Faced with having to apply for a mutual legal assistance treaty (MLAT), which could take years to process, DDA Savik has to settle for building a strong local case, even though she suspects Noonien may be storing content that could greatly increase his sentence. The officers on the ICAC task force reassure her that they're working on a way to access the network connecting the dark device and congratulate her on a job well done.

The European Union's recent efforts to improve its citizens' privacy left out a key demographic—its children. The ePrivacy Directive was designed to bolster the GDPR (General Data Protection Regulation) by protecting "certain online communication services, like webmail or messaging

---

[43] *See United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018) (holding that even if constitutional violation exists, the *Leon* good faith exception precludes suppression, noting a judicial disinclination to find a technique "facially deficient" where legality is questionable and law enforcement sought the prior advice of legal counsel); *see also United States v. Michaud*, No. 3:14-CR-05351, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016) (finding that although the search warrant facially violated the "letter" of the law, it did not violate the "spirit" of the law).

[44] *See United States v. Matish*, No. 4:16-CR-16, 2016 WL 3545776 (E.D. Va. June 23, 2016) (holding that probable cause supported the issuance of the NIT warrant because the affidavit outlined several discrete, voluntary steps an individual must take to access Playpen, described the relevant information, and detailed the website's homepage and registration terms); *United States v. Darby*, No. 2:16-CR-36, 2016 WL 3189703 (E.D. Va. June 3, 2016) (denying defendant's motion to suppress due to law enforcement appropriate collection of evidence over a lengthy period of time and summarized findings in a detailed affidavit, filed the warrant with the federal district with closest connection, and gathered limited information via warrant); *United States v. Epich*, No. 15-CR-163, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016) (concluding that the search warrant possessed adequate information to meet the particularity requirement, including such details as the targeted individuals for the search, information obtained, time frame for information sought by the warrant, how the warrant would be used, and additional attachments that further described the warrant).

[45] *See United States v. Jean*, 207 F. Supp. 3D 920 (2016) (holding that the Playpen protocols, including the operations of TOR software and network, the obviousness of Playpen's contraband nature from the website's home screen which contained an image of partially clothed children, the website's emphasis on anonymity and alias usage, and the numerous steps required by users to create a profile and log in, all culminated to demonstrate the defendant's intent to access child sexual abuse material).

[46] *See United States v. Werdene*, 883 F.3d 204 (2018); *United States v. Horton*, 863 F.3d 1041 (2017); *United States v. Workman*, 863 F.3d 1313, 1321 (10th Cir. 2017), cert. denied, No. 17-7042, 2018 WL 1786016 (U.S. Apr. 16, 2018); *United States v. Sasiadek*, No. 15-CR-159W, 2017 WL 5019257, at *5 (W.D.N.Y. Nov. 2, 2017); *United States v. Stepus*, 2018 U.S. Dist. LEXIS 25853 (2018); *United States v. Anzalone*, Civ. No. 15-10347-PBS, 2016 WL 5339723 (D. Mass. September 9, 2016).

services." However, it failed to accommodate cloud providers who had been voluntarily processing content or traffic data in order to detect child sexual abuse online.[47] This oversight resulted in a disastrous 58 percent drop in service provider reports of suspected EU-based child abuse to the National Center for Missing and Exploited Children (NCMEC).[48] A new law quickly followed a temporary derogation, allowing cloud service providers to resume voluntary scanning for CSAM but not without considerable controversy.[49]

Similarly, pushback from privacy advocates at least temporarily derailed Apple's plans to enable similar scanning. The "NeuralHash" detection tool was intended to identify CSAM without ever decrypting the images,[50] and Apple would "only [learn] about images that match known CSAM."[51] This new tool had the potential to uncover troves of child sexual abuse material: despite its market share, Apple was responsible for only 265 of the 21,751,085 reports of CSAM made to the NCMEC CyberTipline in 2020.[52] However, as in the EU, privacy proponents rallied against the technology and argued that it potentially could be used to track political dissidents' or journalists' messages. John Carr, secretary of the UK Children's Charities' Coalition on Internet Safety, worries that privacy advocates' stance is "highly theoretical," and calls for children's advocates to more closely engage with and educate their privacy-oriented counterparts.[53] An outcry against hypothetical nightmare scenarios obstructed Apple's policies addressing the current reality of rampant online sexual exploitation of children.

Prosecutors can exercise leadership in educating courts and others on how technology can be used to safeguard the rights of private citizens in the course of a criminal investigation. Other countries' laws can be instructive to this end. One report, for example, found that many laws provide for law enforcement or intelligence services "to obtain access to encrypted communications or the means of decryption under certain circumstances."[54]

The EncroChat case is one example, but from an international standpoint, another recent FBI operation may be more salient. Beginning in 2018, the agency took the concept behind its Playpen operation a step further: they acquired an EncroChat-like messaging app called Anom, and

---

[47] EUROPEAN COMMISSION, "Fighting child sexual abuse: Commission proposes interim legislation to enable communications services to continue detecting child sexual abuse online," September 10, 2021, available at https://digital-strategy.ec.europa.eu/en/news/fighting-child-sexual-abuse-commission-proposes-interim-legislation-enable-communications-services (last accessed September 25, 2021).
[48] NCMEC, "A Battle Won, But Not the War in the Global Fight For Child Safety," April 29, 2021, available at https://www.missingkids.org/content/ncmec/en/blog/2020/we-are-in-danger-of-losing-the-global-battle-for-child-safety.html (last accessed September 25, 2021).
[49] Clothilde Goujard, "EU Parliament lets companies look for child abuse on their platforms, with reservations," POLITICO, July 6, 2021, available at https://www.politico.eu/article/european-parliament-platforms-child-sexual-abuse-reporting-law/ (last accessed September 25, 2021).
[50] Patrick Howell O'Neill, "Apple defends its new anti-child-abuse tech against privacy concerns," MIT TECHNOLOGY REVIEW, August 6 2021, available at https://www.technologyreview.com/2021/08/06/1030852/apple-child-abuse-scanning-surveillance/ (last accessed September 25, 2021).
[51] APPLE INC., "Expanded Protections for Children," September 3, 2021, available at https://www.apple.com/child-safety/ (last accessed October 18, 2021).
[52] ECPAT INTERNATIONAL, "Children's Groups Express Strong Support for Apple's New Policy," available at https://ecpat.org/wp-content/uploads/2021/09/Apple-letter-final-220921-rev.pdf (last accessed October 18, 2021).
[53] Goujard, *supra*.
[54] Law Library of Congress Global Legal Research Directorate, "Government Access to Encrypted Communications," May 2016, available at https://tile.loc.gov/storage-services/service/ll/llglrd/2016591728/2016591728.pdf (last accessed September 25, 2021).

collaborated with the Australian Federal Police (AFP) and other agencies to decrypt messages, identify hundreds of suspects, and seize both drug and cash assets. The complicated operation required the FBI to simultaneously operate like—and appear to be—a legitimate startup business *and* meet numerous legal requirements.[55] Owning the messaging system enabled the FBI to create a backdoor to monitor otherwise encrypted communications without users' knowledge.[56]

The operation was enabled in large part by the enactment of Australia's Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA),[57] which doesn't go as far as requiring service providers to build deliberate "back door" vulnerabilities or to prevent providers from repairing a vulnerability; but rather, it allows Australian law enforcement to request any one of a number of other workarounds, including the substitution of a service, as they did with the FBI's Anom app. In addition, Australian agencies can assist other countries' law enforcement "so far as those laws relate to serious foreign offences."[58]

For U.S.-based prosecutors, applying practical measures to international policy may not be feasible except at the federal level. On the other hand, as more countries enact legislation like TOLA or bilateral treaties allowing them to cooperate with U.S. CLOUD Act requirements (Australia enacted preliminary legislation to this end in summer 2021),[59] avenues may open to a greater number of state and local prosecutors, too.

However, the UK's existing and Australia's forthcoming bilateral treaties stand alone globally, due in large part to the European Union's GDPR. Negotiations for an electronic evidence-sharing agreement between the U.S. Department of Justice and the European Commission have been ongoing since 2019.[60]

---

[55] Joseph Cox, "'We Have to Run a Good Company': How the FBI Sold Its Encryption Honeypot." VICE, June 9, 2021, available at https://www.vice.com/en/article/m7e733/anom-fbi-andrew-young-encryption-honeypot (last accessed September 25, 2021).
[56] Campbell Kwan, "AFP used controversial encryption laws in its 'most significant operation in policing history'," ZDNET, June 7, 2021, available at https://www.zdnet.com/index.php/forums/disc/index.php/article/australias-encryption-laws-used-by-afp-in-countrys-most-significant-operation-in-policing-history/ (last accessed September 25, 2021).
[57] *Id.*
[58] Stilgherrian, "What's actually in Australia's encryption laws? Everything you need to know," ZDNET, December 19, 2018, available at https://www.zdnet.com/article/whats-actually-in-australias-encryption-laws-everything-you-need-to-know/ (last accessed September 25, 2021).
[59] Alexander Berengaut, Kiley Naas, & Jim Garland, "Australia Passes Cross-Border Data Access Law, Creates a Pathway for CLOUD Act Bilateral Agreement." COVINGTON INSIDE PRIVACY, July 2, 2021, available at https://www.insideprivacy.com/cross-border-transfers/australia-passes-cross-border-data-access-law-creates-a-pathway-for-cloud-act-bilateral-agreement/ (last accessed September 25, 2021).
[60] Eugenia Lostri, "The CLOUD Act," CENTER FOR STRATEGIC & INTERNATIONAL STUDIES, October 2, 2020, available at https://www.csis.org/blogs/technology-policy-blog/cloud-act (last accessed September 25, 2021).

Conclusion

At the policy level, experts recognize the need for privacy but recommend a measured government approach to "going dark." The central coordination of lawful hacking investigations and prosecutions "involving the use of sensitive government tools, novel network investigative techniques, or where a single warrant is expected to result in prosecutions in numerous but unidentified jurisdictions"[61] would allow the government to "focus on obtaining the clearest possible answers, and not fear establishing unfavorable precedents."[62] In addition, limiting lawful hacking to be used only to investigate the most serious cases—including child exploitation—"ensures appropriate allocation of research and development resources, better protects tools, and facilitates coordinated prosecution strategies."[63] But "mass hacking" many computers at once, as in the European Union's 2020 takedown of the EncroChat network,[64] is not out of the question if "the Justice Department [can] clearly articulate how warrants for such operations can satisfy all constitutional requirements."[65]

Modern child exploitation poses significant technological hurdles, but progress in combating this atrocity must not come solely from tools and technologies. Though common sense and traditional investigative skills are also key in these cases,[66] perhaps the most critical predictor of success in the fight against online child exploitation is the creativity and resolve of child advocates. Legal and technological opportunities and setbacks occur rapidly and unpredictably, but as the quote often attributed to Winston Churchill indicates: "Success is not final, failure is not fatal: it is the courage to continue that counts."

---

[61] Susan Hennessey, "Lawful hacking and the case for a strategic approach to 'Going Dark,'" BROOKINGS INSTITUTE, October 7, 2016, available at https://www.brookings.edu/research/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark (last accessed November 5, 2021).
[62] *Id.*
[63] *Id.*
[64] Joseph Cox, "Encrypted Phone Network Says It's Shutting Down After Police Hack," VICE, June 22, 2020, available at https://www.vice.com/en/article/5dz9qx/encrochat-hacked-shutting-down-encrypted-phone (last accessed August 24, 2021).
[65] Hennessey, *supra*.
[66] Robert J. Peters, Technology-Facilitated Child Abuse, in Robert Geffner, Victor Vieth, Viola Vaughan-Eden, Alan Rosenbaum, Kevin Hamberger & Jacqueline White (Eds), Handbook of Interpersonal Violence Across the Lifespan (2020).