a program of zero abuse PROJECT

Judge, Jury… Service Provider?

TiPP

6 Strategies for Prosecutors Confronting Objections from Electronic Service Providers

By Joseph Remy, Katherine Hansen, Abigail Abraham, Robert Peters & Christa Miller

A search warrant is a court order: once a judge signs it, the person or entity it's served on is legally bound to comply. However, when dealing with Big Tech, sometimes even a judge's signature isn't compelling enough to force action. The parameters of data privacy are a topic of hot debate.

That debate often centers around how provider-held data has been commoditized—routinely collected, bundled, and sold in ways that consumers don't fully understand. But this data trove has also become central to diverse criminal investigations, both horrific and mundane. As a result, law enforcement's demand and reliance on electronic service providers is increasing.[1]

Responding to concerns raised by privacy advocates, providers have sought to make the data harder for the government to obtain. One way they do so is by pushing back on legal process.[2] According to a 2013 blog, Google "frequently" reviews search warrants and "may refuse to provide the information or seek to narrow the request."[3]

These internal reviews and resulting back-and-forth correspondence can then delay or stymie investigations. With forethought and careful planning, however, you can head off this pushback and more promptly procure the digital evidence necessary to prove your case.

Crafting efficient service provider requests on an ongoing basis boils down to six main strategies:

1. **Know what you're asking for**, why you need it, and your legal grounds for getting it.
2. **Educate judges, service providers, and investigators** on the nature and value of the data.
3. **Customize your boilerplates.**
4. **Assume good faith** when there's a delay, but handle delays and denials expeditiously.
5. **Plan your budget.** (Yes, many providers—especially major ones—charge for data processing!)
6. **Seek notification of unreturned responsive records.**

---

[1] Binder, Matt. "U.S. government requests for Google user data up 510% since 2010, report says." Mashable, June 16, 2020. https://mashable.com/article/google-facebook-government-user-data-study/ accessed 11 March 2021.
[2] *Developments in the Law — More Data, More Problems*, 131 Harv. L. Rev. 1715, 1722 (2018). https://harvardlawreview.org/2018/04/cooperation-or-resistance-the-role-of-tech-companies-in-government-surveillance/ accessed 11 March 2021.
[3] Drummond, David. "Google's approach to government requests for user data." The Keyword Blog, Google. January 27, 2013. https://blog.google/technology/safety-security/googles-approach-to-government-requests/ accessed 24 February 2021.

1. Know what you're asking for

All data is not equal and different types of legal process reflect this. How invasive a search could be into private data determines which legal process is required—and the law keeps refining what "invasive" means.

For example, user-generated content (e.g., emails, photographs, text messages) is generally understood to be discrete, private information; therefore, accessing it requires a search warrant. Compare that to real-time location information, which can seem less detailed and intrusive. However, a *history* of location information can generate enough pattern-of-life data to have similar privacy implications to traditional content.[4] Determining that a user visits the same residence most nights of the week indicates a relationship with the occupant in a way that could also be established through text exchanges. Accordingly, significant location data, such as cell site location Information, also requires a search warrant.

Generally, the type of legal process will reflect these variances:[5]

- **Non-content subscriber information**, such as IP address logs, requires only a subpoena.
- **Metadata**—date and time stamps, and other descriptive data—can be obtained with a 2703(d) court order. Typically, metadata is needed to establish timelines, corroborate or refute other evidence, and lend overall context to the content you're seeking.
- **Content**, such as emails, pictures, and messaging, requires a search warrant.
- **Real-time location information** and cell site location information (CSLI) require a search warrant.
- **"Reverse" content**—geofence and keyword searches, which rely on the records of a large number of users to identify suspects based on location or search histories—demands a multi-step search warrant process.

Is it relevant?

The significance of data to an investigation isn't always immediately obvious. That's why an investigation exists—to determine whether the data is relevant. To discover that fact, however, first requires access.

After determining the *type* of data you'd like to request, the next challenge is deciding *how much*. What's the right balance between "enough" data—proportional to the crime being prosecuted as well as the type of evidence requested—and "too much"?

---

[4] Moreover, these definitions can change. Cell site location information (CSLI), for instance, didn't require a search warrant until 2018, when the Supreme Court ruled that intrusive searches could be broad as well as deep (thinking that goes back to 2012). See *Carpenter v. United States*, 138 S.Ct. 2206 (2018); *United States v. Jones*, 565 U.S. 400, 132 S.Ct. 945 (2012)

[5] Legal process in these situations is defined by the Electronic Communications Privacy Act (ECPA) and in particular, its Title II—the Stored Communications Act (SCA). However, some state laws are more restrictive than the federal law, and the SCA's legal process categories are directly in conflict with extensive case law. Notably, California's version, CalECPA—which covers the major electronic service providers based in that state—requires a search warrant to obtain IP address and payment details as well as call detail records. Prudence—and the potential trajectory of case law—dictates that prosecutors and law enforcement follow the maxim "when in doubt, get a search warrant."

For instance, pattern-of-life and attribution data can be relevant and legally significant even when not directly related to the offense. Those contextual details can help authenticate other data and establish an association to a suspect, victim, or witness—or even serve as exculpatory material.

The private companies storing the data cannot and should not be involved in the investigative process. They don't have the level of access to case facts that could help them determine which data is relevant, nor is it their legal role. That responsibility lies with government investigators and attorneys, overseen by judges, who set data-collection parameters, review the results for relevance, and then disregard data deemed irrelevant.

> Consider that pattern-of-life and attribution data are relevant and legally significant.

2. Educate judges

Judges aren't usually technology experts, and service providers aren't judges. Yet they share one thing in common: their tendency to push back on "overbroad" search warrants.

A judge who understands how the technology works will be in a better position to decide whether to grant authorization to support an investigation. Because you have to be able to explain why the data you seek comports with the requirements to issue the legal process, you have the opportunity to educate the judge on how it all works.

Take, for example, "reverse" search warrants. Media attention and, to an extent, provider marketing focus on the privacy implications of collecting precision geolocation or keyword search information. These collections could include information from hundreds of unrelated bystanders in protected spaces or activities, e.g., private residences, houses of worship, and protests.

> A judge who understands the technology will better decide whether to support an investigation.

In reality, reverse warrants are typically a two- or three-step process that is designed to narrow a set of anonymized data *before* a fresh search warrant asks for any personal identifying or private information. The process takes time, but it's a good-faith effort to minimize the scope of intrusion or the number of people whose privacy is impacted. Helping a judge understand the protections built into the process enables them to rule effectively on whether the intrusion is warranted and comports with legal requirements.

A further example would be a request for a large volume of data related to a particular individual. Capturing all data related to a suspect from the day of the crime could reveal additional victims or accomplices across service providers. On the other hand, asking for more data—even with probable cause to obtain it—also means added time for both procuring and examining the results.

For this reason, it's helpful to explain in the warrant affidavit why the complete range of data is necessary—to corroborate what was on the device, fill in blanks in the event that device data was deleted or is missing, or distinguish "normal" from unusual patterns of life. Expounding on your reasoning provides the necessary nexus between the evidence sought and the probable cause required to obtain it.

Missing from much of the discussion about overbreadth is the need to capture exonerating information.

Providing an explanation is particularly important in cases where specific dates or ranges are not possible, such as typical child exploitation cases. Abused children are unlikely to recall the precise dates and times for each (or any) of the dozens of sustained sexual assaults they have endured, and expecting them to do so is both unreasonable and unrealistic. Even demanding that an adult recall the precise timing and circumstances of their last 50 sexual encounters would be futile. Framing the absurdity of such a requirement for the judiciary may be necessary to explore the full scope of potential evidence—incriminating or exculpatory.

Exculpatory material

Missing from much of the discussion about overbreadth is the need to capture exonerating information. Although some judges prefer to see dates limiting a search warrant to data from only the day of the crime—or ranges to include only a few days before and after the offense—it's better to avoid overbreadth by tailoring the parameters of the request to a specific need for information. It should be noted that overly limiting timeframes risks the loss of both exculpatory and Inculpatory Information.

3. Customize your boilerplates

Using boilerplate language in search warrant templates saves work in terms of "reinventing the wheel" and can be an efficient use of time. However, this shortcut can backfire in a rapidly evolving industry.

That's not just owing to scrivener's errors—like an incorrect IP address, date and time range, or other data mistake that could result in actual overreach of an innocent person or protected data. Overreliance on boilerplate language can also result in using inaccurate or incomplete language that isn't applicable to the data available—causing you to miss critical information.

To that end:

- Most providers, especially large ones, have law enforcement liaisons. Build relationships with these people, who can help you select appropriate terminology and facilitate your requests.

As a U.S. Justice Department publication points out: "Communication is necessary because every network provider works differently."[6]

- Similarly, communicating with providers can also help you educate law enforcement officers on the verbiage necessary to obtain the evidence being sought. A provider might exclude some requested information simply because the language used in the warrant is inconsistent with provider-specific language. For example, depending on the scrutiny of the provider, simply requesting relevant "photographs and associated data" may not yield exchangeable image file format (EXIF) data containing, among other things, the latitude and longitude of where the photograph was taken.

> "Communication is necessary because every network provider works differently." –USDOJ

- Use provider-specific templates. Different providers have different requirements.
- Review both provider templates and internal templates (such as for a search warrant) on a regular basis to ensure the data you seek is consistent with the data currently available.
- Remember to include language for nondisclosure orders in cases involving ongoing investigations or other delay-notice circumstances.[7]
- As a matter of due diligence—regardless of whether it is required by office policy—review case-specific warrants, too, when they come back from investigators but before they're presented to a judge. Watch for changes to template language, and be sure that boilerplate explanations are tied to the facts that support probable cause for the offense.

4. Assume good faith but handle delays promptly

Assume good faith when dealing with delays…

While delays are undoubtedly frustrating to law enforcement seeking to advance an investigation, a delay isn't the same as pushback, and may even be inadvertent rather than intentional.

For example, a smaller provider may be under-resourced, lacking the personnel or legal knowledge to manage government requests. Submissions can also be improperly handled or processed, and the warrant will need to be resubmitted.

Regardless of the reason for the delay, a service provider may respond well to a courteous reminder email or phone call from the detective investigating the case:

> A service provider may respond well to a courteous reminder email or phone call from the detective investigating the case.

[6] Jarrett, H. Marshall, Michael W. Bailie, Ed Hagen, Nathan Judish. "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." U.S. Department of Justice Office of Legal Education, Executive Office for United States Attorneys. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf accessed 15 February 2021

[7] 18 U.S.C. § 2705. https://www.law.cornell.edu/uscode/text/18/2705 accessed 14 March 2021.

- The provider's law enforcement liaison is likely dealing with many other cases, and you don't know how they log (or search) their requests. Your reminder should include as much information about the case as you can provide: the date the request was submitted, what kind of request it was (e.g., warrant or subpoena), and any case number generated by their law enforcement portal.
- Coordinate who will be responsible for follow-ups—the investigator or prosecutor. (Note: if the case has been filed with your prosecutor's office, this is your responsibility.)
- Document the correspondence in the case file: the date and time you made contact and/or whom you contacted or spoke with. If you leave a voicemail, make a note about its content. These details could be important later on.

…But handle delays and denials expeditiously

Depending on the jurisdiction and its applicable statutes and rules, providers that object to a court order, subpoena, or search warrant based on its validity or authority may have the right to request judicial review from the judge who signed the order. In particular:

- The California Electronic Communications Privacy Act (CalECPA), passed in 2015, allows providers as well as targets to petition the issuing court "to void or modify the warrant, order, or process" if it violates either the state or U.S. constitutions.[8]
- The 2018 U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act amended the federal ECPA, providing 14 days to move to modify or quash, and only in specific circumstances such as seeking information from nondomestic accounts.[9]

Overly long delays or outright refusals demand more than polite reminders. By contravening a court order, a provider's delay or refusal technically may usurp judicial authority and therefore be in contempt of court. However, steps can be taken in between a reminder and an order of contempt.

What's a "lengthy delay"? Many state statutes grant limited periods of time—typically 10 to 14 days—for providers to produce records. Based on the circumstances, your search warrant may include a request for a shorter time period. Otherwise, when submitting the appropriate legal process for data, the investigator should obtain an expected return date from the service provider.

> **Although a provider's delay or refusal may be in contempt of court, steps can be taken in between a reminder and an order of contempt.**

Know your state's "shot clock" as well as the clock in the state where the provider is located. If a first reminder call is ignored or not received well, the follow-up can include a gentle reminder of the shot clock, the expected return date the provider offered, or the time period in the warrant itself.

[8] SB-178 Privacy: electronic communications: search warrant. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB178 accessed 12 March 2021.
[9] 18 U.S.C. § 2703(h)(2). https://www.law.cornell.edu/uscode/text/18/2703 accessed 27 February 2021.

If a warrant is refused:

- Investigate the objection,
- Educate service providers and investigators, and
- File a Motion to Compel or Order to Show Cause.

Investigate the objection

In cases where the provider hasn't reached out to the investigator, or the investigator has resubmitted a search warrant only to encounter more resistance, it's worth finding out the basis for the refusal to comply.

A denial or objection may be based not on statutory requirements but instead on the provider's perception—or even their own behind-the-scenes investigation. In that case, it may be possible to file legal process on the provider for information about their investigation.

Educate service providers and investigators, too

Like judges, sometimes a provider may push back because they don't understand what overbreadth means in the warrant's context, including the evidentiary necessity of authentication and attribution of the requested data.

Other times, a provider's pushback may be based on concern about whether the warrant is technically compliant with statutory requirements or whether it creates an undue burden for them to obtain the data.

Either way, providers generally make a point to contact the detective who submitted the warrant, explaining any perceived technical insufficiency. They reach out particularly when they will not be providing records covered by the warrant or if the warrant does not include a nondisclosure order.

This outreach creates an opportunity for you to educate them. You or the investigator can explain why the warrant is valid and why they are legally required to comply. Sometimes, especially when dealing with lawyers representing smaller ISPs or other service providers, it's simply a matter of explaining the Stored Communications Act (SCA).[10] Other times, it may actually be necessary to submit a warrant that is in accordance with the statute in question.

File a Motion to Compel

When informal negotiations fail and the provider remains unmoved, the next step is to secure the production of the requested records via state or federal judiciary. Judicial authority to compel compliance—and sanction a provider for failing to comply—is an elemental power derived from constitutional, statutory, and court rules. Pursuing this route typically means filing a Motion to Compel or a similar legal instrument.

---

[10] 18 U.S.C. Chapter 121 §§ 2701-2712. https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121 accessed 13 March 2021.

18 U.S.C. 2703(d) does provide for service providers to seek to "quash or modify [a court] order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider."

Whether this exception extends to search warrants is a matter of some debate. CalECPA says it does. However, in 2017 two years after CalECPA's enactment, a New York state appeals court declined to consider that question. Although it stated (in stark contrast to the dissenting opinion in the case) "the SCA plainly distinguishes between subpoenas and warrants, and there is no indication that Congress intended for SCA warrants to be treated as subpoenas," it rejected the provider's motion to quash.[11]

> **Judicial authority to compel compliance is an elemental power derived from constitutional, statutory, and court rules.**

It likewise rejected the provider's Motion to Compel to review the affidavit supporting probable cause for the warrant. The court reasoned neither motion was valid because both orders were not "civil in nature" and therefore unappealable. In ruling on that technicality, the court also declined to consider whether providers had the "standing to assert Fourth Amendment claims on behalf of its users."[12]

Seek an Order of Contempt

A rather drastic remedy, an Order of Contempt should be viewed as a last resort after all other remedies have been exhausted. Following the filing of an Order to Show Cause (not to be held in contempt), the Order of Contempt is a formal declaration that a party—in this case, an electronic service provider—has violated a court directive and is subject to penalty.

The penalty could be financial or could otherwise impede the provider's ability to perform certain actions. Therefore, both the law enforcement professional and electronic service provider should exercise due caution before turning to such a remedy.

> **An Order of Contempt should be viewed as a last resort after all other remedies have been exhausted.**

If a service provider is uncooperative, the situation demands an immediate letter of preservation under the SCA, which provides for electronic records to be preserved for 90 days upon request.[13]

Submitting a letter of preservation is a minimally intrusive way to ensure that potential evidence won't be lost or destroyed while investigators are waiting on a search warrant. By using the service, the user has

[11] In re 381 Search Warrants to Facebook, Inc., 78 N.E.3d 141 (NY 2017). https://law.justia.com/cases/new-york/court-of-appeals/2017/16.html accessed 15 February 2021
[12] *Id.*
[13] 18 U.S.C. Chapter 121 § 2703(f) https://www.law.cornell.edu/uscode/text/18/2703 accessed 13 March 2021.

already consented to the preservation, which isn't in itself a search or seizure.[14] And the user can continue to interact normally with their account without affecting potential evidence: even if a user deletes an item, it is not erased within the service provider's records. In addition, because a 2703(d) order is a snapshot of a point in time, anything the order doesn't capture going forward—any new content—*can* be permanently deleted by the user.

Some legal scholars believe preservation upon request does in fact constitute a seizure. "Preservation triggers a Fourth Amendment seizure because the provider, acting as the government's agent, takes away the account holder's control of the account," wrote Orin Kerr.[15] Further, a 2703(f) preservation order "circumvents privacy protections by avoiding judicial oversight, is relied upon excessively…and constitutes a seizure."[16]

Can a preservation letter be "overbroad"?

Delays or refusals from a provider can be problematic because providers save some data, like geolocation information, for a shorter period of time. Additionally, no law codifies a mandatory retention period for data, so company policies vary and can change at will with no notice.

Kerr's remedy is that the "government can continue to use the Internet preservation statute in a limited way, such as to freeze an account while investigators draft a proper warrant application," but it would otherwise need a warrant. This proposal, however, does not appear distinct from the language in 2703(f) or its typical application.

Kerr's opinion also contravenes years of authority allowing law enforcement to detain personal property, pending a search warrant, even without reasonable suspicion to believe it contains evidence or contraband. Similarly, preservation requests may often wind up broader than the resulting search warrant.

5. Plan your budget

The evolution of technology since the SCA's enactment in 1986 has made the *process* of production much more efficient. However, the *volume* of government requests for data in the form of legal process has increased dramatically as well. This increase in activity is especially apparent when reviewing legal transparency reports from providers like Dropbox, Google, and Verizon.

To manage government requests, service providers have expanded their legal compliance departments and leveraged technology that reduces the time and effort associated with accessing and compiling data.

---

[14] Tadayon, Armin. "Preservation Requests and the Fourth Amendment." *Seattle University Law Review*, Vol. 44:105. 2020. https://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=2717&context=sulr accessed 15 February 2021.
[15] Kerr, Orin. "The Fourth Amendment Limits of Internet Content Preservation." *St. Louis University Law Journal* (forthcoming). December 18, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3751094 accessed 15 February 2021.
[16] Tadayon, *Id.*

Still, companies won't undertake these activities without a government order. Additionally, some activities, like cell site analysis, are both outside the norm of most requests and more burdensome in general to carry out.

As a result, the SCA provides for remote computing or electronic communications services to recoup from governments the costs "directly incurred in searching for, assembling, reproducing, or otherwise providing" data in response to requests.[17] State statutes may also allow for similar reimbursement. (Whether these policies effectively monetize privacy protection is a subject for a different article.)

Can a service provider withhold data records pending payment? 18 U.S.C. § 2706's plain wording suggests not.

Under 18 U.S.C. 2706(b), service providers and governments are to come to mutual agreement around the amount to be reimbursed. If they don't, the court that signed off on the legal process (or the court in the jurisdiction adjudicating the criminal action under investigation) decides the amount.

Under 18 U.S.C. 2706(c), however, telecommunication carriers are exempted from seeking cost reimbursement for subscriber and toll records and listings—routine requests that demand little effort.[18]

Can a service provider withhold data records pending payment? 18 U.S.C. § 2706's plain wording suggests not. Specifically, its reliance on the word "reimburse" suggests that the records will already have been produced, and the statute merely offers a way for the provider to recoup associated costs.

Further, according to the July 2002 edition of the U.S. Department of Justice Computer Crime and Intellectual Property Section, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations III (D)(5): "ECPA makes clear Congress's intent to authorize the use of § 2703 search warrants for subscriber content as a form of *compulsory* process directed to third-party network providers—not as a traditional search warrant."[19] [Emphasis added.]

A later edition of that same publication offers further guidance on reimbursement practices, limiting providers to recoup only those expenses directly related to production: "In practice, if the service provider seeks what appears to be unreasonably high reimbursement costs, the government should demand a detailed accounting of costs incurred by activity."[20]

---

[17] 18 U.S.C. Chapter 121 § 2706 https://www.law.cornell.edu/uscode/text/18/2706 accessed 13 March 2021.
[18] See, e.g., *Michigan Bell Telephone Co. v. Drug Enforcement Administration*, 693 F.Supp. 542 (E.D.Mich. 1988). https://law.justia.com/cases/federal/district-courts/FSupp/693/542/2357208/ accessed 14 March 2021.
[19] "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." Computer Crime and Intellectual Property Section, Criminal Division, U.S. Department of Justice. July 2002. https://www.thecre.com/fedlaw/legal8/s_smanual2002.htm accessed 15 February 2021.
[20] Jarrett, *Id.*

6. Seek notification of unreturned responsive records

Regardless of whether service providers turn over records without much pushback or you need to file a Motion to Compel or Order to Show Cause, ensuring you got what you asked for is a final step in due diligence.

In other words, perform a quality check. Not only should you ensure the production content matches the username on both the warrant and the affidavit, you also should ensure the provider has responded with everything included in the warrant.

Data validation, however, may prove difficult. Data storage and management practices, the formatting of warrant returns, and how often that all changes are proprietary—and therefore opaque.

> Ensuring you got what you asked for is a final step in due diligence.

Technology like Google Takeout or Facebook archives may help. Implemented (or refined) to meet the requirements of the European Union's General Data Protection Regulation (GDPR),[21] these tools allow you to compare the data you received in a warrant return to the data requested. However, these data comparisons take time and effort—and may not encompass critical information like metadata.[22]

Just as you can include language in your search warrant ordering the provider *not* to notify their user of the search, you can also incorporate language requiring the provider *to* notify you if they do not provide fully responsive records. Notification requirements not only can help prevent inadvertent omission of documents, but they also give the requestor better standing when communicating with the service provider about any oversights.

Conclusion

Given the obstacles to obtaining data from service providers, it's fair to ask: is it worth the effort? After all, corporate legal teams can appear bigger and better prepared next to an overextended county prosecutor. On the other hand, encrypted devices, retracted witness statements, and other challenges often render third-party data pivotal in child exploitation cases.

[21] Conger, Kate. "How to Download Your Data With All the Fancy New GDPR Tools." Gizmodo, May 25, 2018. https://gizmodo.com/how-to-download-your-data-with-all-the-fancy-new-gdpr-t-1826334079 accessed 14 March 2021.
[22] Patzakis, John, & Botta, Brent. "Facebook Download Your Information Function Omits Significant Amounts of Evidence." X1 Next Gen GRC & EDiscovery Law Blog, October 19, 2020. https://www.x1.com/2020/10/19/facebook-download-your-information-function-omits-significant-amounts-of-evidence/ accessed 14 March 2021.

Rather than play the role of a judge, electronic service providers and law enforcement alike should create an open dialogue in resolving disputes to protect both victims and the platforms themselves from harmful criminal activity. And if that dialogue breaks down, law enforcement and prosecution should not hesitate to avail themselves of proper legal mechanisms. Seeking justice for victims and preventing future offenses are well worth the effort.

 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.