The court is not filing this document at this time
Received
D. Peal
2-24-20

Jennifer Granick, Bar No. 168423
ACLU Foundation
39 Drumm Street
San Francisco, CA 94111
415-343-0758
jgranick@aclu.org

Jacob A. Snow, Bar No. 270988
ACLU Foundation of Northern California
39 Drumm Street
San Francisco, CA 94111
415-621-2493
jsnow@aclunc.org

Peter Bibring, Bar No. 223981
Mohammad Tajsar, Bar No. 280152
ACLU Foundation of Southern California
1313 West 8th Street
Los Angeles, CA 90017
213-977-5295
pbibring@aclusocal.org
mtajsar@aclusocal.org

On the brief:
Brett Max Kaufman
Alexia Ramirez
Nathan Freed Wessler
ACLU Foundation
125 Broad Street, 18th Floor
New York, NY 10004
212-549-2500
bkaufman@aclu.org
aramirez@aclu.org
nwessler@aclu.org

Attorneys for Amici Curiae American Civil Liberties Union and American Civil Liberties Union of Northern and Southern California in Support of Petitioner

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF LOS ANGELES

IN RE SEARCH WARRANT TO GOOGLE FOR ALL RECORDS ASSOCIATED WITH GOOGLE ACCOUNT SCOTTARCLA@GMAIL.COM	Case No. 20CCPC0020 **[PROPOSED] BRIEF OF AMICI CURIAE ACLU, ACLU OF SOUTHERN CALIFORNIA, AND ACLU OF NORTHERN CALIFORNIA IN SUPPORT OF MOTION TO QUASH SEARCH WARRANT**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. Since its founding in 1920, the ACLU has frequently appeared before the Supreme Court and other federal courts in numerous cases implicating Americans' right to privacy in the digital age, including as counsel in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and as amicus in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

The ACLU of Southern California and the ACLU of Northern California ("ACLU of Northern and Southern California") are two California state affiliates of the national ACLU. The ACLU of Northern and Southern California participate in a statewide Technology and Civil Liberties Project, founded in 2004, which works specifically on legal and policy issues at the intersection of new technology and privacy, free speech, and other civil liberties and civil rights. The ACLU of Northern and Southern California supported the passage of CalECPA and served as key advisors to the law's authors, Senators Mark Leno and Joel Anderson, throughout the legislative process. Accordingly, amici are uniquely positioned to provide the Court with a comprehensive perspective on the purpose and meaning of CalECPA.[1]

[1] Amici would like to thank Jacob Apkon and Thomas McBrien, students in the Technology Law & Policy Clinic at NYU School of Law, for their significant contributions to this brief.

INTRODUCTION

The Founders may not have foreseen the advanced technologies of the digital age, but they drafted the Fourth Amendment to forbid warrants like the one at issue in this proceeding. The central motivation behind the ratification of the Fourth Amendment was to ensure that government officials could not invade the privacies of a person's life without justification, restraint, and oversight. The amendment rejected the "general warrant," an imperial legal instrument granting the government unrestrained authority to rummage through people's lives under cover of governmental power.

The warrant that Sergeant Richard Biddle obtained for Scott Budnick's Google account data is a vast departure from what the Fourth Amendment permits. Officer Biddle sought every scrap of information in Mr. Budnick's account from the account's inception. A legal demand to seize all the paper records someone had created over the years would be an impermissible general warrant, forbidden by the Fourth Amendment and reviled by the framers. *Stanford v. Texas*, 379 U.S. 476, 482–83 (1965) (describing warrants that "authorized . . . the arrest and seizure of all the papers of a named person thought to be connected with a libel" as a type of general warrant). Today, such court orders are even more pernicious. Americans in 1792 did not generate anything close to the volume of information that ordinary people today store on phones, computers, and in the "cloud."

The astounding amount of digital information subject to seizure and search presents serious challenges for privacy. Seizure of the contents of an entire online account can reveal an astonishingly complete record of an individual's life—private papers, reading lists, appointment books, correspondence, photographs, location history, research interests, and more. In many cases, even seizures that appear at first glance to be narrowly framed would give police huge quantities of irrelevant and private information. But courts have the necessary tools to ensure that warrants for electronic information are not general warrants, either on their face or in effect. First, courts must limit "intentional over-seizures." Warrants to third parties such as Google or Facebook should be cabined to only relevant categories of data for a defined time period, as supported by probable cause. The warrant in this matter utterly failed that test. Second, even

when investigators must over-seize electronic data for pragmatic reasons, warrant-issuing courts can and should require officers to conduct searches in a manner designed to uncover relevant evidence and avoid rummaging through irrelevant personal matters. Courts could impose search protocols, or require officers to document their searches to ensure an opportunity for effective judicial oversight. With modern forensic tools, there is no need for law enforcement officers to randomly open files on a hard drive. Searches can target relevant actors, keywords, or time frames so as not to be overbroad. Courts could require "clean teams" or special masters to segregate relevant from irrelevant information, or require the government to forego application of the plain view doctrine so as not to take advantage of overbroad searches. The goals of these limitations are fundamental to the Fourth Amendment: to cabin law enforcement discretion, prevent searches from straying beyond their justifications, protect privacy, and limit the risk of abuse. And when violations of the Fourth Amendment occur, as in this case, expungement of improperly seized or searched information is a necessary and proper remedy.

While the Fourth Amendment requires quashal here, Officer Biddle's warrant is also an egregious violation of the California Electronic Communications Privacy Act ("CalECPA"). That law, which took effect in January of 2016, established clear statutory protections for Californians' privacy rights when a government entity seeks electronic communications and device information. Those protections include concrete particularity requirements and a requirement that the government notify the target. The government met neither requirement here. When the government obtains information in violation of CalECPA, the statute also provides a remedy: suppression of evidence in court and destruction of material unlawfully obtained. Any of Mr. Budnick's information that Officer Biddle obtained from Google should, under CalECPA, be promptly destroyed.

ARGUMENT

I. Online Email And Storage Accounts Like Mr. Budnick's Contain Vast Amounts Of Extremely Sensitive, Private Information.

Digital information generated by today's devices and services reveals individuals' private matters far beyond what one could learn from physical analogs. *See Riley v. California*, 573 U.S.

373, 394 (2014). A device the size of a human palm can store practically unlimited quantities of data. *Id*. For example, sixteen gigabytes of information—the standard capacity of a smart phone several years ago—"translates to millions of pages of text, thousands of pictures, or hundreds of videos." *Id.* Google offers 15 gigabytes of data storage for free, and up to 200 gigabytes of storage at negligible cost. *See About Google One*, Google, https://one.google.com/about. Google's servers store volumes of data, including email, photos, videos, calendar items, documents and spreadsheets, videos watched, search terms entered, websites visited, and the locations users have been to while carrying their phones. These accounts contain people's most intimate and private documents—love notes, tax records, business plans, health data, religious and political affiliations, personal finances, and digital diaries, to name just a few. Today, people who carry cell phones, use social media, or take advantage of online storage generate an almost incomprehensible quantity of sensitive and private information. A search of even one such account is deeply invasive. *See United States v. Payton*, 573 F.3d 859, 861–62 (9th Cir. 2009) ("There is no question that computers are capable of storing immense amounts of information and often contain a great deal of private information. Searches of computers therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers."). Police access to social media accounts and online communications services present a "threat [that] is further elevated . . . because, perhaps more than any other location—including a residence, a computer hard drive, or a car—[they] provide[] a single window through which almost every detail of a person's life is visible." *United States v. Shipp*, 392 F. Supp. 3d 300, 308 (E.D.N.Y. 2019) (describing Facebook).

Moreover, while our garages and desk drawers may fill up with knickknacks, requiring periodic spring cleaning, digital data can pile up and persist indefinitely, meaning law enforcement is capable of accessing years'—and soon, decades'—worth of personal information. *See Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018); *Riley*, 573 U.S. at 394. This combination of volume, depth and longevity of personal information raises strong privacy concerns because in aggregate, digital information reveals much more than the sum of each part. *See Riley*, 573 U.S. at 394.

A warrant like the one at issue here could also subject individuals like Mr. Budnick to abuse and harassment. Casual police access to the incredible variety and volume of personal correspondence and other private information stored in the cloud today could be used to deter lawful political advocacy, or to scare others who wish to engage in advocacy for other issues. Passwords and PIN codes, which the warrant demanded, could be used to spy on account holders, allowing officers access to digital information without judicial oversight. Passwords could also be misused to send fake messages, impersonating the account holder. Location information can reveal personal relationships, religious affiliation, political activity, and health conditions. Stock holdings and financial data could only be of prurient interest under circumstances like those involved in this case.

The staggeringly broad categories of information Officer Biddle sought, and appears to have obtained, from Mr. Budnick's Google account go far beyond what is constitutionally permissible. Officer Biddle asked for categories of information that could not have possibly contained any evidence of the so-called "conspiracy" he was investigating (e.g., *all* images and videos, location history, search history, play store applications, credit card numbers, securities records, and other financial data). As *amici* explain below, Officer Biddle's warrant would violate the Fourth Amendment even if there were probable cause of criminal activity, which there is not.

II. Warrants For Digital Data Must Be Scrupulously Particular and Narrow in Scope In Order To Be Constitutional.

The Fourth Amendment is intended "to place obstacles in the way of a too permeating police surveillance."[2] *Carpenter*, 138 S. Ct. at 2214 (citation and quotation marks omitted). It requires that search warrants particularly describe the places to be searched and the things to be seized (particularity), and prohibits search for or seizure of anything for which there is not probable cause (overbreadth). To protect the highly private and sensitive nature of today's

[2] California Electronic Privacy Act ("CalECPA"), Cal. Penal Code § 1546.1(e) (2017) guarantees Mr. Budnick independent legal rights that were violated in the course of Officer Biddle's investigation. *See infra* Part IV.

electronically stored information, warrants must impose strict restrictions on law enforcement's electronic searches and seizures so as to avoid unnecessary exposure of our intimate details to investigators.

A. The Fourth Amendment Requires That Warrants Clearly Limit What Officers May Seize, And That Searches Are Designed Only To Find Relevant Information.

The Fourth Amendment protects against general warrants, which were "the worst instrument of arbitrary power . . . that ever was found in an English law book." *Stanford*, 379 U.S. at 481 (quoting founding father James Otis). Search warrants must be particular and narrow in scope. *See, e.g., id.* at 485 ("The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another."); *Berger v. New York*, 388 U.S. 41, 58 (1967) ("The Fourth Amendment's requirement that a warrant 'particularly describ(e) the place to be searched, and the persons or things to be seized,' repudiated these general warrants and 'makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another.'" (alteration in original)); *Groh v. Ramirez*, 540 U.S. 551, 557 (2004) ("[T]he warrant . . . was deficient in particularity because it provided no description of the type of evidence sought."); *Kentucky v. King*, 563 U.S. 452, 459 (2011) ("a warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity."); *People v. Kraft*, 23 Cal.4th 978, 1041 (2000) (citing *Andresen v. Maryland*, 427 U.S. 463, 480 (1976)).

"Specificity has two aspects: particularity and breadth. Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based." *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006) (citations omitted). A warrant is sufficiently particularized only if "nothing is left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927); *see also United States v. Cardwell*, 680 F.2d 75 (9th Cir. 1982); *People v. Frank*, 38 Ca. 3d 711, 724 (1985) (The particularity requirement is

met "if the warrant imposes a meaningful restriction upon the objects to be seized."). The warrant must also constrain invasive "fishing expeditions" by authorizing searches only for evidence of a crime for which there is probable cause. *See Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

A search is unlawfully general where the accompanying warrant "left to the executing officers," rather than to the magistrate upon issuance, "the task of determining what items fell within broad categories stated in the warrant" and where there were no clear guidelines distinguishing between property which was subject to search and that which was not. *United States v. Hillyard*, 677 F.2d 1336, 1339 (9th Cir. 1982) (citing *United States v. Drebin*, 557 F.2d 1316, 1322–23 (9th Cir. 1977)); *see also United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995) (warrant listing fourteen categories of business records without limiting descriptions such as names of companies involved in illegal scheme was not sufficiently particular); *United States v. Stubbs*, 873 F.2d 210, 211 (9th Cir. 1989) (lack of probable cause to seize all office documents without reason to believe tax evasion permeated defendant's entire business).

For example, in *Burrows v. Superior Court*, investigators obtained a warrant to search the office of an attorney accused of misappropriating a client's funds for "all books, records, accounts and bank statements and cancelled checks of the receipt and disbursement of money and any file or documents referring to [four named individuals]." 13 Cal. 3d 238, 241, 248 (1974) (quotation marks omitted). The California Supreme Court held the search unreasonable because the warrant's description of the things to be seized was so broad as to authorize a general search and seizure of the attorney's financial records without limiting the seizure to documents regarding the specific persons allegedly involved in the crime. *Id*. at 250 (objecting to the phrase "any file or documents").

Similarly, in *Aday v. Superior Court*, the court invalidated a warrant to search for nineteen general categories of documents such as checks, sales records and records connected with the petitioner's business. 55 Cal.2d 789, 796 (1961). The court unanimously held the warrant was fatally overbroad:

> Articles of the type listed in general terms in the warrant are ordinarily innocuous and are not necessarily connected with a crime. The various categories, when taken together, were so sweeping as to include virtually all personal business property on the premises and placed no meaningful restriction on the things to be seized. Such a warrant is similar to the general warrant permitting unlimited search, which has long been condemned.

Id. These principles should be even more strictly adhered to when officers are conducting searches of digital information.

B. Overbreadth And Particularity Are Especially Important When Officers Seek Access to Digital Information.

In the age before computers, the particularity requirement was relatively easily understood as applied during searches of physical spaces. For example, a valid warrant to search for a rifle in someone's home does not allow officers to open a medicine cabinet where a rifle could not fit. *See, e.g.*, *Horton v. California*, 496 U.S. 128, 141 (1990).

Today, those physical distinctions are no longer a guide. Computer hard drives and online services contain huge amounts of personal information, both irrelevant material and, potentially, evidence of criminal behavior. Computers typically contain much information outside the scope of any particular criminal investigation. As a result, the digital age requires courts to take even greater care when balancing law enforcement interests with privacy, otherwise digital searches could "become a vehicle for the government to gain access to data which it has no probable cause to collect." *United States v. Comprehensive Drug Testing, Inc.* (*CDT*), 621 F.3d 1162, 1177 (9th Cir. 2010) (per curiam). The need to search large quantities of electronic records "creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *Id*. at 1176.

How should courts deal with these dueling values: law enforcement's legitimate need to search for evidence of a crime on one hand, and the countervailing prohibition against general warrants and their evils on the other? While the answer in any given case will of course be fact-specific, the Fourth Amendment's originating principles are more important than ever as guides.

As technology lowers the barriers to extreme privacy invasions and investigatory overreach, the Fourth Amendment must play a critical role in ensuring that the longstanding balance between the power and authority of the state and the privacy and liberty of the individual

does not, either suddenly or through creep, fall constitutionally out of whack. The Fourth Amendment's bedrock principles are especially necessary where these technological innovations facilitate "a too permeating police surveillance." *Carpenter*, 138 S. Ct. at 2214; *see also Berger*, 388 U.S. at 56 ("The need for particularity . . . is especially great in the case of eavesdropping" because such surveillance "involves an intrusion on privacy that is broad in scope."). In some cases, technology has also given law enforcement the ability to obtain previously unobtainable information. *Carpenter*, 138 S. Ct. at 2217–18. In cases involving law enforcement's use or exploitation of emerging technologies, the Fourth Amendment analysis asks whether the police conduct threatens to disrupt the traditional "relationship between citizen and government in a way that is inimical to democratic society." *United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (quotation marks omitted). This analysis "is informed by historical understandings 'of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted.'" *Carpenter*, 138 S. Ct. at 2214 (alteration in original) (quoting *Carroll v. United States*, 267 U.S. 132, 149 (1925)); *see also Kyllo v. United States*, 533 U.S. 27, 34 (2001). Courts must ensure that technological innovation does not allow the government to encroach on the degree of privacy the Fourth Amendment was adopted to protect. *See Carpenter*, 138 S. Ct. at 2214 (cell-site location information); *Kyllo*, 533 U.S. at 34 (thermal imaging).

III. Courts Can Craft Warrants To Constrain Invasive Rummaging—A Risk With Even Seemingly Limited Descriptions of Information.

The point at which an officer seeks a warrant is the best chance a court has to protect individual privacy interests from unconstitutional invasions. Nothing can truly restore the confidentiality and integrity of the details of a person's life once police have combed through their correspondence and other data. There will very rarely be a case where the probable cause showing can justify an officer's request for an "all-content" warrant. Nor are such warrants necessary as a practical matter; service providers can turn over far more tailored sets of data, narrowing by type of data, date range, conversation participants, or other variables dictated by probable cause.

That is not to say that anything short of an "all-content" warrant will satisfy the Constitution. Police seizure of more limited categories of digital information may risk unconstitutionally overbroad searches and seizures as well. Because electronic storage generally intermingles responsive and non-responsive data, there is a risk of violating expectations of privacy in files unrelated to the crime under investigation. In order to ensure that familiar Fourth Amendment principles remain effective when police conduct such searches, the Ninth Circuit has recommended that courts implement procedures "to maintain the privacy of materials that are intermingled with seizable materials, and to avoid turning a limited search for particular information into a general search of office file systems and computer databases." *CDT*, 621 F.3d at 1170. Courts can either impose search conditions at the outset, or can carefully review investigators' searches after the fact to ensure that the search was narrowly tailored to probable cause. If an illegal seizure or search has taken place, the appropriate remedy must include deletion of all data impermissibly seized. *Id.* at 1177 (the government should return materials that were not the object of the search once they have been segregated).

In sum, courts have tools at hand to manage the dangers of overbroad warrants.

A. Seizures should be limited to relevant categories of information.

There is no need for, and the Fourth Amendment does not allow, "all-content" warrants demanding seizure of whatever account content or digital files might exist. Rather than issue "all-content" warrants, courts should only authorize seizure of relevant categories of data. For example, in one federal investigation of an illegal firearms charge, a search warrant to Facebook demanded all personal information, activity logs, photos and videos from the user as well as those posted by others that tag the suspect, all postings, private messages, and chats, all friend requests, groups and applications activity, all private messages and video call history, check-ins, IP logs, "likes", searches, use of Facebook Marketplace, payment information, privacy settings, blocked users, and tech support requests. *Shipp*, 392 F. Supp. 3d at 303–06. This list was not limited to the types of information likely to provide evidence of the specific crime under investigation. The district court expressed "serious concerns regarding the breadth of [the] Facebook warrants," pointing out that many of the categories of information were irrelevant to

probable cause. *Id.* at 307. Moreover, the social media company was in the position to discriminate between relevant and irrelevant categories of information. The FBI had no need to seize, for example, Marketplace transaction logs on the grounds that relevant evidence could be found there. *Id.* at 310.[3]

Similarly in *United States v. Wey*, the Southern District of New York held that two warrants identifying categories of often generic items subject to seizure failed the Fourth Amendment's particularity requirement. 256 F. Supp. 3d 355 (S.D.N.Y. 2017). Those categories included all "financial records, notes, memoranda, records of internal and external communications, correspondence, audio tapes[] and video tapes, [and] photographs," among others. *Id.* at 386 (quotation marks omitted). The only limitation as to the search and seizure was that the documents had to pertain to the suspects. But because every document seized from the suspect pertains to the suspect, the court held that the warrants did not impose "meaningful parameters on an otherwise limitless search of a defendant's electronic media" and they failed "to link the evidence sought to the criminal activity supported by probable cause" *Id.* at 387. Thus, the warrants did "not satisfy the particularity requirement." *Id.*

Courts should authorize seizure of only those categories of data likely to contain evidence of the crime.

B. Seizures should be limited by time frame and other available characteristics.

Warrants can easily limit data seizures from online providers by time frame. If an offense allegedly took place in 2019, police may not need to obtain email from any other year, never mind from the inception of the account, as it did here. *See United States v. Abboud*, 438 F.3d 554, 576 (6th Cir. 2006) ("Failure to limit broad descriptive terms by relevant dates, when such dates are available to the police, will render a warrant overbroad." (citations omitted)); *United States v. Diaz*, 841 F.2d 1, 4–5 (1st Cir. 1988) (warrant overbroad when authorized seizure

[3] Where a social network is the data custodian, concerns that a suspect could effectively disguise responsive data are relatively minor. *See Shipp*, 392 F. Supp. 3d at 309–10. Still, the *Shipp* court overstated a suspect's capacity to effectively hide evidence from officers, given today's sophisticated data analysis tools.

records before the first instance of wrongdoing mentioned in the affidavit); *In re [REDACTED]@gmail.com*, 62 F. Supp. 3d 1100, 1104 (N.D. Cal. 2014) (no warrant issued where government did not include a date limitation); *In re Search of Google Email Accounts identified in Attachment A*, 92 F. Supp. 3d 944 (D. Alaska 2015) (application without date restriction denied as overbroad).

When available, courts can and should also use other criteria of digital information to constrain police and ensure that seizures are scoped to probable cause. *See United States v. Griffith*, 867 F.3d 1265, 1276 (D.C. Cir. 2017) (deeming a warrant's failure to narrow a search based on ownership of a cell phone to be insufficiently particular). For example, if conversations between Mr. Budnick and either the Los Angeles Probation Department or the Sheriff's Department were genuinely potential evidence of a crime, the warrant could demand that Google turn over only his messages with the relevant government email addresses. *In re Search of Info. Associated With Four Redacted Gmail Accounts*, 371 F. Supp. 3d 843, 845 (D. Or. 2018) (warrant for all emails associated suspect's account is overbroad because Google is able to disclose only those emails the government has probable cause to search). Similarly, Google Photos is designed to do image searches. *About Google Photos*, Google, https://www.google.com/photos/about/ (explaining that photos saved to Google photos "are organized and searchable by the places and things in them – no tagging required"). Investigators might seize from Google only those photos that were taken at a particular location or contain a particular person of interest.

C. Searches Must Be Limited By Probable Cause, And Should Use Clean Teams, Data Deletion, And Other Tools To Protect Privacy.

In some circumstances, investigators will necessarily over-seize electronic data. Even a well-scoped warrant for social media data or email accounts will include some irrelevant and innocent information. Often, officers can justify the removal of computers or cell phones from the scene of a crime—over-seizing the data stored there.[4] Where over-seizure is unavoidable,

[4] The Ninth Circuit requires the affidavit to explain why practical constraints might require the

courts can and should issue warrants that ensure that law enforcement's subsequent searches of that data will be cabined to probable cause.

The Ninth Circuit in *CDT* suggested limitations courts can impose on search warrants for intermingled data. *See* 621 F.3d at 1169–71 (opinion of the court); *id.* at 1178–80 (Kozinski, C.J., concurring) (suggesting limits on retention of unresponsive data, abandonment of the "plain view" doctrine, and protections for the privacy rights of third parties whose data is intermingled).

For example, courts can consider whether to impose a search protocol in the warrant, or whether to review the search after-the-fact to ensure that it was scoped to probable cause. *See, e.g.*, *In re Search Warrant*, 71 A.3d 1158, 1184 (Vt. 2012); *CDT*, 621 F.3d at 1178–79. The Ninth Circuit, for example, has expressed a preference for a search protocol, but even in its absence, "[t]he reasonableness of the officer's acts both in executing the warrant and in performing a subsequent search of seized materials *remains subject to judicial review*." *Hill*, 459 F.3d at 978 (9th Cir. 2006) (emphasis added) (citation omitted).

A warrant-issuing court might require the use of independent review teams to "sort[], segregat[e], decod[e] and otherwise separat[e] seizable data (as defined by the warrant) from all other data," so as to shield investigators from exposure to information beyond the scope of the warrant. *CDT*, 621 F.3d at 1179. Another tool is to require the use of search technology, including "hashing tools," to identify responsive files "without actually opening the files themselves." *Id.* at 1179 (Kozinski, C.J., concurring).

Yet another option is to require police to "waive reliance upon the plain view doctrine in digital evidence cases," full stop. In other words, the government must agree not to take advantage of its own unwillingness or inability to conduct digital searches in a particularized manner. *Id.* at 1180. Regardless of the method chosen, however, the searches "must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents." *Id.* at 1180 (Kozinski, C.J., concurring).

---

seizure of the entire computer system for off-site examination. *See Hill*, 459 F.3d at 975–76 (stating that the affidavit must "demonstrate to the magistrate factually why such a broad search and seizure authority is reasonable in the case at hand").

Contrary to some government claims, officers need not perform a file-by-file review of the data on a suspect's computer in every case. Some prosecutors have argued and some courts have held that because criminals can hide or mislabel files, expansive searches of digital information are both practically necessary and permissible under the Fourth Amendment. *See, e.g.*, *United States v. Stabile*, 633 F.3d 219, 237 (3d Cir. 2011); *see also United States v. Williams*, 592 F.3d 511, 521 (4th Cir. 2010). But these decisions are premised on an outmoded understanding of today's technology. Indeed, review of every file in suspects' online accounts or on their hard drives will often be counterproductive, for it is impractical for an investigator to manually review the hundreds of thousands of images, files, and messages stored there.

> An acquired hard drive may contain hundreds of thousands of data files; identifying the data files that contain information of interest, including information concealed through file compression and access control, can be a daunting task. In addition, data files of interest may contain extraneous information that should be filtered. For example, yesterday's firewall log might hold millions of records, but only five of the records might be related to the event of interest.

See Karen Kent et al., *Guide to Integrating Forensic Techniques Into Incident Response: Recommendations of the National Institute of Standards and Technology*, No. 800-86 at § 3.2, U.S. Dep't of Commerce (Aug. 2006), https://perma.cc/Y2N7-K65R.

Instead, modern forensics tools, widely available today for both criminal investigations and e-discovery, can search data for file type, dates, and keywords, all without revealing the contents of non-responsive documents to a human reviewer.

> Fortunately, various tools and techniques can be used to reduce the amount of data that has to be sifted through. Text and pattern searches can be used to identify pertinent data, such as finding documents that mention a particular subject or person, or identifying e-mail log entries for a particular e-mail address. Another helpful technique is to use a tool that can determine the type of contents of each data file, such as text, graphics, music, or a compressed file archive. Knowledge of data file types can be used to identify files that merit further study, as well as to exclude files that are of no interest to the examination. There are also databases containing information about known files, which can also be used to include or exclude files from further consideration.

Id. Some tools can search for categories of images based on the machine's guesses about what a photo contains. For example, the Blacklight tool can categorize both still images and videos.

Their categories are: Alcohol, Child Sexual Abuse Material (CSAM), Currency, Drugs, Extremism, Gambling, Gore, Porn, Swim/Underwear, and Weapons.[5]

In some cases, when a suspect is using sophisticated techniques to hide data, it may make sense to give officers increased leeway in their search to find potentially hidden information. But in such a scenario, there should be a probable cause showing of the actor's "sophisticated" nature—perhaps, for example, the suspect is a skilled computer programmer who knows how to manipulate data. But since the scope of a warrant must be limited by probable cause, if a suspect is not sophisticated, there may be no reason to believe that relevant evidence will be found in otherwise innocent-seeming places. And even if such concerns apply to search of a suspect's own electronic device, they are unlikely to apply to a search of data stored by Google or Facebook, which structure data storage in ways that make sophisticated concealment difficult. *See Shipp*, 392 F. Supp. 3d at 308 (discussing the vast and complex nature of Facebook data).

Finally, even when a search is reasonable, the government should be required to delete materials that were not the object of the search once they have been segregated. *See CDT*, 621 F.3d at 1177 (discussing need to segregate nonresponsive information). Expungement is essential in cases such as this one where the officer's search and seizure were unconstitutionally overbroad. *See, e.g.*, *Fazaga v. FBI*, 916 F.3d 1202, 1239 (9th Cir. 2019) ("We have repeatedly and consistently recognized that federal courts can order expungement of records, criminal and otherwise, to vindicate constitutional rights."); *Maurer v. Pitchess*, 691 F.2d 434, 437 (9th Cir. 1982) ("It is well settled that the federal courts have inherent equitable power to order 'the expungement of local arrest records as an appropriate remedy in the wake of police action in violation of constitutional rights.'" (citation omitted)).

Courts now are implementing versions of these solutions. For example, in Vermont, magistrates may design and supervise "targeted searches" by "restricting law enforcement's search to those items that met certain parameters based on dates, types of files, or the author of a

[5] *BlackBag Announces Release of BlackLight 2019 R2*, BlackBag (Sept. 5, 2019), https://www.blackbagtech.com/press-releases/blackbag-announces-release-of-blacklight-2019-r2.

document." *See In re Search Warrant*, 71 A.3d at 1184; *see also In re [REDACTED]@gmail.com*, 62 F. Supp. 3d at 1104 (denying a search warrant for a particular email account because "there is no date restriction of any kind").

And a recent district court case from Michigan helpfully illustrates how courts are now confronting these issues. In *United States v. Stetkiw*, the government insisted, and the court was concerned, that, "individuals might hide information in a way that forces a protocol-bound investigator to overlook it." No. 18-20579, 2019 WL 2866516, at *5 (E.D. Mich. July 3, 2019). Nevertheless, the court held that "an *ex ante* 'minimization' requirement can address concerns about potential Fourth Amendment violations of protocol-less searches, with a goal of decreasing the amount of non-responsive [electronically stored information] encountered in a search." *Id.* (citing Emily Berman, *Digital Searches, the Fourth Amendment, and the Magistrates' Revolt*, 68 Emory L.J. 49, 55 (2018)). The court concluded that *ex ante* procedures would have several advantages:

> First, it can minimize the need for ex post review of those procedures, which is often contentious as parties debate motions to suppress evidence in criminal cases. Second, it allows a magistrate judge to closely work with the Government to ensure its preferred procedures do not violate the Fourth Amendment. Third, it can promote the development of case law that can distinguish permissible and impermissible procedures to better protect Fourth Amendment rights. Finally, it could prevent situations where certain file locations are authorized for search by warrant, but the practical implications of that authorization create a general warrant without the magistrate judge's knowledge.

Id. While the *Stetkiw* court did not maintain that *ex ante* protocols must be required in every case, it did suggest that in order to escape such protocols, the government "should demonstrate that the level of probable cause to search [electronically stored information] is high enough to justify a search without minimization." *Id.*

Fourth Amendment–compliant searches and seizures not only protect privacy, but serve law enforcement interests by focusing searches on their proper objects and relevant evidence. Indeed, one of the biggest problems that officers encounter in investigations involving electronic data is that they have too much data to make sense of. At the same time, particularity and overbreadth limitations may be an inconvenience for law enforcement. That is, in part, the point. As one federal judge put it, "[i]t is almost always possible to characterize the Fourth Amendment

as an inconvenience to law enforcement officials as they carry out their vital duties," but "[t]hat inconvenience . . . is one of the fundamental protections that separates the United States of America from totalitarian regimes." *Doe v. Prosecutor*, 566 F. Supp. 2d 862, 887 (S.D. Ind. 2008). *See also Johnson v. United States*, 333 U.S. 10, 15 (1948); *United States v. Morgan*, 743 F.2d 1158, 1163–64 (6th Cir. 1984); *United States v. Diggs*, 544 F.2d 116, 130 (3d Cir. 1976).

IV. The Warrant for Mr. Budnick's Google Account Violates CalECPA, and Everything Provided In Response Should Be Destroyed.

Under California law, Officer Biddle's warrant in this case was illegally overbroad and all materials obtained pursuant to the warrant must be destroyed.

A. CalECPA Provides Strong, Clear Digital Privacy Rules For Government, Companies, And The Public.

California has a long tradition of providing more robust privacy protections than federal law. CalECPA continues that tradition. Passed in 2015, CalECPA establishes clear rules to protect Californians' privacy rights when a government entity seeks electronic communications and device information.

First, CalECPA requires a probable-cause warrant for all electronic information and device information, including information sought from third-party service providers or from personal electronic devices. Cal. Penal Code § 1546.1(a)(2), (a)(3). Under CalECPA, law enforcement and other California government entities must obtain a warrant to demand people's electronic information. This includes everything from emails, digital documents, and text messages to location and medical information.[6]

Second, CalECPA specifies the degree of detail that a warrant must contain. Warrants must "describe with particularity the information to be seized by specifying, as appropriate and reasonable, the time periods covered, the target individuals or accounts, the applications or

[6] People also have strong privacy interests in the metadata—which is fully protected by CalECPA—associated with their accounts, devices, and information. *See generally Metadata: Piecing Together a Privacy Solution*, ACLU of N. Cal. (2014), available at https://www.aclunc.org/sites/default/files/Metadata%20report%20FINAL%202%2021%2014%20cover%20%2B%20inside%20for%20web%20%283%29.pdf.

services covered, and the types of information sought." Cal. Penal Code § 1546.1(d)(1). CalECPA includes heightened particularity requirements specifically because online services and devices house vast amounts of personal information. As a result, a warrant that permits the search of a device or online service threatens to intrude upon the privacy not just of the user of the online service or the holder of the device, but also upon countless others. CalECPA recognizes that, to effectively protect people's electronic privacy, the *warrant itself* must restrain the reach of the government's power to intrude into our most private digital spaces.

Third, CalECPA requires that the government entity must provide notice to the target of any warrant that is contemporaneous with the execution of the warrant. *Id.* § 1546.2(a)(1). While it is possible for the government to delay that notice, the factual showing required to do so is extraordinary, limited to circumstances where sworn testimony demonstrates a risk of endangering life, enabling flight from prosecution, or tampering with evidence or witnesses. *Id.* § 1546.2(a)(2); *Id.* § 1546.2(b)(2) (defining "adverse result"). And delays, when granted, are limited to 90 days, with court approval necessary for each extension. *Id.* § 1546.2(b)(2).

Finally, a core provision of CalECPA is its clear and robust remedies, including both suppression of evidence and destruction of material obtained in violation of the law. The suppression remedy is available whenever CalECPA's rules are violated. Cal. Penal Code § 1546.4(a). But even before a suppression motion can be filed, CalECPA provides that affected individuals may petition the court to void the warrant and order destruction of "any information obtained in violation of [CalECPA], or the California Constitution, or the United States Constitution." *Id.* § 1546.4(c).

B. The Search Warrant Failed to Comply with CalECPA.

The search warrant in this case violated CalECPA's bright-line rules governing the particularity with which information subject to seizure must be specified and appears to violate the mandatory provision for notice to targeted individuals.

1. The Warrant to Mr. Budnick Violates CalECPA's Particularity Requirement.

The warrant in this case seeks "[a]ll records associated with" Mr. Budnick's Google Account. Search Warrant for Scott Budnick's Google Account, Pet. Ex. A, at BS000002. The warrant then lists, at extraordinary length, examples of information associated captured by that phrase. The provided list includes essentially every piece of private, sensitive, intimate, or personal information fathomable: every username, all account activity, every password, every text message, every email, every physical location (no matter the source), every calendar entry, every personal contact, every document, every piece of financial information, every photograph, every mobile app, every search, every call, and every purchase. This is exactly the "virtual current biography" that the California Constitution protects, and that motivated the authors of CalECPA to put strong protection for electronic information into the law.[7]

The statute is explicit that warrants shall describe with particularity, "as appropriate and reasonable, the time periods covered . . . , the applications or services covered, and the types of information sought." Cal Penal Code § 1546.1(d)(1). The overbroad warrant in this case, by sweeping in every piece of information from the target account, without limitation, is the reason CalECPA exists; there can be no clearer violation of the statute's command that warrants to service providers be narrowly tailored and particular.

Even the list of examples, if it were read to be limiting, violates CalECPA. The warrant's command that Google produce every piece of information from "[i]nception of account to the

[7] *See People v. Chapman*, 36 Cal.3d 98, 108–109 (1984); Bill Analysis, Assembly Committee on Privacy and Consumer Protection 9–10, SB 178 (June 23, 2015) ("SB 178 updates existing federal and California statutory law for the digital age and codifies federal and state constitutional rights to privacy and free speech by instituting a clear, uniform warrant rule for California law enforcement access to electronic information, including data from personal electronic devices, emails, digital documents, text messages, metadata, and location information. Each of these categories can reveal sensitive information about a Californian's personal life: her friends and associates, her physical and mental health, her religious and political beliefs, and more. The California Supreme Court has long held that this type of information constitutes a 'virtual current biography' that merits constitutional protection. SB 178 would codify that protection into statute. SB 178 also ensures that proper notice, reporting, and enforcement provisions are also updated and in place for government access to electronic information and to ensure that the law is followed.").

date this warrant is signed" fails to include reasonable particularity with respect to the time periods covered, as the statute mandates. Def. Ex. A, at BS000002; *see also* Cal Penal Code § 1546.1(d)(1). And in requesting "[a]ll applications downloaded, installed, and/or purchased by the associated account and/or device" the warrant additionally fails to specify the "applications or services covered," opting instead to seize every application. Def. Ex. A, at BS000003; Cal Penal Code § 1546.1(d)(1).

CalECPA was written with the threat of unlimited warrants like the one in this case in mind. As the author wrote, "Law enforcement is increasingly taking advantage of outdated privacy laws to turn mobile phones into tracking devices and to access emails, digital documents, and text messages without proper judicial oversight."[8] Importantly, CalECPA protects not just people, but the companies who operate services for consumers in California. Those companies, as the author highlighted, "are increasingly concerned about the loss of consumer trust and its business impact, and are in need of a consistent statewide standard for law enforcement requests."[9] If warrants like the one in this case are allowed, consumer trust in both service providers and government will be further undermined.

For these reasons, CalECPA puts in place statutory mandates limiting law enforcement access to exactly the sources of information at issue here, and it demands strict judicial oversight when those mandates are not followed.

2. Mr. Budnick May Not Have Received Notice Required by CalECPA.

CalECPA also inaugurated a powerful and detailed notice regime commanding law enforcement to inform targets of investigations when warrants are executed. The notice requirements under CalECPA go far beyond mere clerical or procedural requirements and create new and important rights for individuals whose information is captured by law enforcement pursuant to a warrant.

---

[8] Bill Analysis, Assembly Committee on Public Safety 12, SB 178 (July 14, 2015).

[9] *Id.* at 13.

As the legislature recognized explicitly, CalECPA's notice requirements go beyond federal law, under which "a governmental entity is not required to provide notice to a subscriber or customer when a warrant is obtained for specified electronic information." Bill Analysis, Privacy: Electronic Communications: Search Warrants 7, Senate Committee on Appropriations, SB 178 (April 22, 2015). These new individualized notice rights were a central focus of the legislature because of their significant fiscal impact. *Id.* Both the requirement that the target individual be notified in ordinary circumstances when the warrant is executed, *and* the requirement that even more detailed notice be provided when the original notice is delayed, were carefully considered by the legislature and determined to be worth the cost.[10] In sum, CalECPA created new, strict, and powerful notice rights for the targets of warrants in California.

All targets of a warrant must, under ordinary circumstances, receive notice contemporaneously with the execution of the warrant. Cal. Penal Code § 1546.2(a)(7). That notice can be delayed, but for no longer than 90 days at a time, and each such delay requires separate court authorization. *Id.* § 1546.2(b)(1). If the government obtains a delay, the statute requires that the later notice be even more extensive. In addition to notifying the target that the warrant has been executed, any notice provided after a period of delay must also include "a copy of all electronic information obtained or a summary of that information, including, *at a minimum*, the number and types of records disclosed, the date and time when the earliest and latest records were created, and a statement of the grounds for the court's determination to grant a delay in notifying the individual." *Id.* § 1546.2(b)(3) (emphasis added).

[10] Bill Analysis, Assembly Committee on Appropriations 1–2, SB 178 (May 28, 2015) ("[U]nder existing federal law, a governmental entity may require a provider of electronic communication service to disclose a record or other information pertaining to a subscriber to or customer of such service under specified circumstances, including pursuant to a warrant or court order. A governmental entity receiving records or information under this provision of federal law is not required to provide notice to a subscriber or customer." (citing 18 USC § 2703)).

C. Because This Warrant Violated CalECPA, All Materials Officers Obtained Pursuant to the Warrant Must Be Destroyed.

Independent of the Fourth Amendment (which requires the same result in this case), CalECPA explicitly provides robust remedies to people whose information is unlawfully obtained by the government. First, any material obtained in violation of CalECPA is subject to suppression under Section 1546.4(a). Second, anyone whose information is targeted by the warrant can petition the court to void or modify the warrant or order destruction of the unlawfully obtained evidence. Cal. Penal Code § 1546.4(c).

These two remedies ensure that anyone affected by an illegal warrant has a remedy under CalECPA to address the harm. When unlawfully obtained material is sought to be introduced into evidence, it must be suppressed. Cal. Penal Code § 1546.4(a). But information that is not used in court still implicates important privacy interests. CalECPA protects those interests by empowering affected individuals to petition the court to modify the warrant or destroy the unlawfully collected information.[11]

Because the warrant represents an egregious violation of CalECPA's particularity requirement, and because the government also appears to have violated the notice requirement, the Court should order that all information received pursuant to the warrant be destroyed.

CONCLUSION

For the reasons stated above, amici support Mr. Budnick's motion to quash the search warrant issued for his Google account information. Mr. Budnick should get notice as required by CalECPA, and the investigators in this case should be required to destroy all the data they may have received as a result of the warrant.

In addition, in future cases involving the search or seizure of electronic information, whether in an online account or on a phone or computer hard drive, issuing judges in this court

[11] *See Saunders v. Superior Court*, 12 Cal. App. 5th Supp. 1, 22–23 (Cal. App. Dep't Super. Ct. 2017) (discussing the public policy concerns motivating CalECPA, including protecting private electronic device information and noting that the legislation "provides additional privacy protections to this kind of information—like notice, time limits, and sealing provisions—reflecting the recognized heightened privacy concerns in both cell-phone records and content").

could take advantage of the tools at their disposal to ensure that these types of investigations are particular and narrow, and do not cross over into the territory of general warrants.

Dated: February 24, 2020

Jennifer Granick, Bar No. 168423
ACLU Foundation
39 Drumm Street
San Francisco, CA 94111
415-343-0758
jgranick@aclu.org

Jacob A. Snow, Bar No. 270988
ACLU Foundation of Northern California
39 Drumm Street
San Francisco, CA 94111
415-621-2493
jsnow@aclunc.org

Peter Bibring, Bar No. 223981
Mohammad Tajsar, Bar No. 280152
ACLU Foundation of Southern California
1313 West 8th Street
Los Angeles, CA 90017
213-977-5295
pbibring@aclusocal.org
mtajsar@aclusocal.org

On the brief:
Brett Max Kaufman
Alexia Ramirez
Nathan Freed Wessler
ACLU Foundation
125 Broad Street, 18th Floor
New York, NY 10004
212-549-2500
bkaufman@aclu.org
aramirez@aclu.org
nwessler@aclu.org