12-240-cr

IN THE

United States Court of Appeals

FOR THE SECOND CIRCUIT

UNITED STATES OF AMERICA,

Appellee,

v.

STAVROS M. GANIAS,

Defendant-Appellant.

On Rehearing En Banc, Appeal from the United States District Court for the District of Connecticut

BRIEF OF GOOGLE INC.
AS AMICUS CURIAE SUPPORTING DEFENDANT-APPELLANT

Todd M. Hinnen

PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101-3099
Telephone: 206.359.8000
Facsimile: 206.359.9000
Email: thinnen@perkinscoie.com

Amanda Andrade

PERKINS COIE LLP
700 13th Street NW, Suite 600
Washington, DC 20005-3960
Telephone: 202.654.6200
Facsimile: 202.654.6211
Email: aandrade@perkinscoie.com

CORPORATE DISCLOSURE STATEMENT

Google Inc. has no parent corporation and no other publicly held corporation owns 10% or more of its stock.

Respectfully submitted,

By:/s/ Todd M. Hinnen
Todd M. Hinnen
Attorney for Amicus Curiae Google Inc.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

FEDERAL CASES

FEDERAL: STATUTES, RULES, REGULATIONS, CONSTITUTIONAL PROVISIONS

OTHER AUTHORITIES

STATEMENT OF INTEREST[1]

Google Inc. is a diversified technology company. Google's mission is to organize the world's information and make it universally accessible and useful. Google offers a variety of web-based products and services, including Search, Gmail, Google+, Maps, YouTube, and Blogger, that are used by people throughout the United States and around the world. Google receives legal process from government authorities and private interests all over the world. Google believes strongly in protecting the privacy of its customers and in being transparent with them to the maximum extent permitted by law about the legal process it receives.

Google's efforts to protect user privacy, promote transparency, and comply with applicable laws are complicated by increasing requests from law enforcement for customer data and legal uncertainty regarding the proper response to these requests. Each year, Google receives thousands of search warrants for user data. In the last several years, the number of warrants Google has received has grown steadily, from less than 1,900 in the latter half of 2012 to over 3,000 for the same

[1] All parties have consented to the filing of this brief. No counsel for a party authored this brief in whole or in part, and no person other than *amicus* or its counsel has made a monetary contribution intended to fund the preparation or submission of the brief.

six-month period in 2014.[2] All together in 2014, Google received more than 6,000 search warrants for information on more than 11,000 user accounts.

Period Ending	Legal Process	User Data Requests	Percentage of requests where some data produced	Users/ Accounts Specified
12/31/2012	Search Warrant	1896	88	3152
6/30/2013	Search Warrant	2456	81	4281
12/31/2013	Search Warrant	2537	81	4180
6/30/2014	Search Warrant	3187	84	5849
12/31/2014	Search Warrant	3127	83	5827

Google has no connection to this case or knowledge of the facts beyond those set forth in the panel's decision, but it has a strong interest in the resolution of the Fourth Amendment issues in this case. Google, like other service providers, may be compelled to disclose user information that upon later review the government determines to be outside the scope of a warrant. A rule allowing the government to retain such user information indefinitely and search it for evidence of unrelated crimes would affect the rights of Google and its users.

SUMMARY OF ARGUMENT

Google's users have a reasonable expectation of privacy, protected by the Fourth Amendment, in the content they store with Google. The government therefore cannot compel Google to disclose users' content without first obtaining a

[2] *See* Google, Transparency Report, http://www.google.com/transparencyreport/userdatarequests/.

warrant based upon a showing of probable cause specifically describing the user account to be searched and the items to be seized. To avoid violating the Fourth Amendment, the government's treatment and handling of user content obtained pursuant to such a warrant must at all times be reasonable.

The panel correctly held that it was unreasonable for the government to retain data the government itself concluded fell outside the scope of the original warrant and to search that over-seized data for evidence of crimes not specified in the original warrant. Google urges the en banc Court to reach the same conclusion as the panel.

If it does not, however, Google urges the en banc Court to recognize certain significant differences between searches and seizures of physical storage media seized during the search of a residence or business and those directing a provider to assist the government in searching and seizing user data stored with that provider (referred to herein as "provider-assisted searches"). As explained below, provider-assisted searches pertain to data held by providers on behalf of users, not to physical storage media seized during searches of residences or businesses, and they are executed differently. When conducting such searches the government often can, and to comply with the Fourth Amendment therefore must, describe the items to be seized from the provider with greater particularity by providing objective

criteria (for example, by identifying a specific online service, specific file types, and specific date ranges) to prevent unnecessary over-seizures.

The government also can and therefore must correct for any unavoidable over-seizure by deleting data obtained as a result of a provider-assisted search that is outside the scope of the warrant. The concerns that may exist in physical search cases about authenticating the remaining data on a forensic image do not apply to data produced by a provider. Even if the en banc Court determines that the government's treatment of Ganias's files and documents was reasonable, it should limit its holding to the facts of this case because the Fourth Amendment may require a different result when the government seizes non-responsive files and documents as the result of a provider-assisted search.

ARGUMENT

I. THE FOURTH AMENDMENT PROTECTS USER CONTENT STORED WITH AN ONLINE SERVICE PROVIDER

A. Users Have a Reasonable Expectation of Privacy Protected by the Fourth Amendment in Content Stored by Online Service Providers.

This case concerns how the Fourth Amendment protects electronic data from unreasonable search or seizure by the government. Although the data at issue in this case was stored on physical storage media seized during a search of Ganias's office, the legal principles that determined the panel's decision apply more broadly

to protect users' reasonable expectation of privacy in electronic data, whether stored on their own physical storage media or, as is increasingly common, with service providers selected by users.

Google is one such service provider. It offers users the ability to communicate via email (Gmail) or real-time text, voice, and video chat (Hangouts); share and collaborate regarding files of various formats, including documents (Google Docs), photographs (Google Photos), and videos (YouTube); and store all of these and other communications and files in Google's online storage infrastructure (Google Drive).

In 2010, the Sixth Circuit held that users have a reasonable expectation of privacy in the communications and files they store with a service provider like Google, and that such communications and files are therefore protected by the Fourth Amendment. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). Other courts have followed *Warshak*. *See, e.g.*, *United States v. Ali*, 870 F. Supp. 2d 10, 39 n.39 (D.D.C. 2012) ("'We recognize individuals have a reasonable expectation of privacy in the content of emails stored, sent, or received through a commercial internet service provider.'") (quoting *United States v. Lucas*, 640 F.3d 168, 178 (6th Cir. 2011) (citing *Warshak*)); *R.S. ex rel. S.S. v. Minnewaska Area Sch. Dist.*, 894 F. Supp. 2d 1128, 1142 (D. Minn. 2012) ("[B]ased on established

Fourth Amendment precedent, . . . R.S. had a reasonable expectation of privacy to her private Facebook information and messages.") (citing cases). Although the Supreme Court has not yet confronted the question, it, too, has recognized that for people in the digital age to "be secure" in their "papers[] and effects," U.S. CONST. AMEND. IV, the protections of the Fourth Amendment must extend to the new online technologies and services that are increasingly the repositories of those papers and effects. *See, e.g.*, *Riley v. California*, 134 S. Ct. 2473, 2491, 2494 (2014) (noting that the search of a cell phone implicates "for many Americans the 'privacies of life'" and that the privacy interest implicated is yet greater when "a search might extend well beyond papers and effects" stored locally on the phone to those stored "in the cloud") (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)); *United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (Fourth Amendment protects the "great deal of information about themselves" people disclose to service providers "in the course of carrying out mundane tasks"). Indeed, users may not even be aware of whether their private papers and effects are stored locally on hardware they possess or remotely on the servers of a service provider. *See Riley*, 134 S. Ct. at 2491 ("Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference.").

Like a computer hard drive, remote storage offered by an online service provider is "akin to a residence in terms of the scope and quantity of private information it may contain." *United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013). Users have a reasonable expectation of privacy in their digital papers and effects, whether stored on their own hard drive or on a virtual drive in a provider's "cloud," and the Fourth Amendment's protections apply in both contexts. Generally speaking, therefore, searches and seizures of electronic evidence in either context must be authorized by a warrant based on a finding of probable cause, must particularly describe the places to be searched and items to be seized, and must be reasonable.

B. The Fourth Amendment Requires that Warrants to Search and Seize Digital Content Be Based on Probable Cause and Describe with Particularity the Places to be Searched and Items to be Seized.

"A warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity." *Kentucky v. King*, 131 S. Ct. 1849, 1856 (2011). This Court has held that to satisfy the particularity requirement, a warrant must: (1) "identify the specific offense for which the police established probable cause"; (2) "describe the place to be searched"; and (3) "specify the items to be seized by their relation to designated crimes." *Galpin*, 720 F.3d at 445-46. It has further held that "a failure to describe

the items to be seized with as much particularity as the circumstances reasonably allow offends the Fourth Amendment because there is no assurance that the permitted invasion of a suspect's privacy and property are no more than absolutely necessary." *United States v. George*, 975 F.2d 72, 76 (2d Cir. 1992).

"The particularity requirement assumes even greater importance" when a warrant authorizes the search and seizure of electronic files because of the volume and variety of private information such files may contain. *Galpin*, 720 F.3d at 446.[3] A warrant that allowed "a search of all computer records without description or limitation," *United States v. Burgess*, 576 F.3d 1078, 1091 (10th Cir. 2009), or failed to state clearly what the government was seeking so that the executing officers could avoid files not described in the warrant, *see United States v. Richards*, 659 F.3d 527, 538 (6th Cir. 2011), would therefore violate the Fourth Amendment.

C. The Fourth Amendment Requires that Each Government Search or Seizure be Reasonable.

To be constitutional, not only must a search and seizure be authorized by a warrant finding that the government has demonstrated probable cause and

[3] A Google user may have accounts for, *inter alia*, email (Gmail), photos (Google Photos), documents (Google Docs), and videos and playlists (YouTube). A warrant for all documents and files associated with a Google user could therefore implicate very different services and types of content associated with nearly every aspect of that person's life.

describing with particularity the places to be searched and items to be seized, the search and seizure must also be reasonable. Because reasonableness is "the ultimate touchstone of the Fourth Amendment," *Brigham City v. Stuart*, 547 U.S. 398, 403 (1996), the manner in which the government executes a warrant must also be reasonable in all respects. *See United States v. Ramirez*, 523 U.S. 65, 71 (1998).

As this Court has repeatedly recognized, the reasonableness requirement of the Fourth Amendment "'not only prevents searches and seizures that would be unreasonable if conducted at all, but also ensures reasonableness in the manner and scope of searches and seizures that are carried out.'" *Lauro v. Charles*, 219 F.3d 202, 209 (2d Cir. 2000) (quoting *Ayeni v. Mottola*, 35 F.3d 680, 684 (2d Cir. 1994)) (internal alterations omitted). Even a search that begins reasonably may become unreasonable if executed improperly. *See, e.g.*, *Wilson v. Layne*, 526 U.S. 603, 611 (1999) ("[I]f the scope of the search exceeds that permitted by the terms of a validly issued warrant or the character of the relevant exception from the warrant requirement, the subsequent seizure is unconstitutional without more."). Where a search entails seizure of information the government subsequently determines to be outside the scope of the warrant, reasonableness requires that the government delete such information or return it to the custodian from whom it was

seized. *See United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1172 (9th Cir. 2010) (noting that returning information outside the scope of the warrant helps preserve the integrity of the business and protect its customers' privacy). In this case, the panel correctly held that it was unreasonable for the government to retain information that the government itself had concluded was outside the scope of the original warrant. *See United States v. Ganias*, 755 F.3d 125, 137 (2d Cir. 2014). If the en banc Court determines that the government's conduct in this case was reasonable, however, the Court should limit its holding to the facts of this case because a provider-assisted search presents different facts that require different treatment of seized data subsequently determined to be outside the scope of a warrant.

II. FOURTH AMENDMENT PRINCIPLES MAY APPLY DIFFERENTLY TO PROVIDER-ASSISTED SEARCHES

The government executes warrants to search and seize data stored with a service provider substantially differently than warrants for data stored locally on physical storage media. Provider-assisted searches generally involve a two-step process in which the provider is compelled to produce a set of communications to the government, and the government must then review them and seize only those communications for which the warrant application established probable cause.

U.S. Department of Justice, Searching and Seizing Computers and Electronic Evidence in Criminal Investigations at 134 & 161 (2009).[4]

Given the unique nature of provider-assisted searches, the Fourth Amendment may require different privacy protections for users who store their content with a service provider than it does for users who store data locally. In the provider-assisted search context, it is particularly important to establish rules that protect documents produced by providers that the government subsequently determines the warrant application did not establish probable cause to seize.

A. The Fourth Amendment May Require Greater Particularity in Warrants Directing a Provider to Assist in Search and Seizure of User Content.

For reasons the panel's decision explains, the government may need to seize computers and other local storage media during the search of a residence, office, or other physical premises. *See Ganias*, 755 F.3d at 135 (noting that seizure of complete images of computers and drives is permitted only "[i]n light of the significant burdens on-site review would place on both the individual and the Government"). The issues associated with on-site review, however, do not apply

[4] Providers can, of course, "cull emails from an email account" where the warrant provides objective criteria that do not require the exercise of discretion; for example, it can "disclos[e] all emails from a particular time period." *In the Matter of a Warrant for All Content and Other Information Associated with the Email Account xxxxxx gmail.com*, 33 F. Supp. 3d 386, 394 (S.D.N.Y. 2014).

to the execution of a warrant that directs a provider to assist the government in the initial search and seizure of stored digital data.

The government need not (and, with rare exception, does not) occupy the business of the provider during the execution of the warrant. *See United States v. Bach*, 310 F.3d 1063, 1066-67 (8th Cir. 2002); U.S. Department of Justice, Searching and Seizing Computers and Electronic Evidence in Criminal Investigations at 134 (2009) ("[I]nvestigators ordinarily do not themselves search through the provider's computers in search of the materials described in the warrant. Instead, investigators serve the warrant on the provider as they would a subpoena and the provider produces the material specified in the warrant."). There is no countervailing privacy interest in minimizing the duration of the government's presence in the private space of the entity subject to search. The provider is generally far more familiar with the data environment to be searched (its services) than law enforcement is with a local data environment composed of computers, hard drives, and other storage media maintained by a user. The provider may maintain, as part of the operation of the service, records regarding the data environment that are not subject to the user's manipulation (for instance, a log of when and from what IP address a user logged into the account), and the

provider may have developed specialized tools for identifying records within that data environment.

For all these reasons, the requirements of particularity and reasonableness may operate differently in a provider-assisted search than they do in the search of local computers and storage media. In a warrant for data stored by a provider, the government will often be able to identify with particularity objective criteria that the provider can apply to narrow the scope of the search, such as the service, type of file, and date range it has probable cause to believe may contain evidence of a crime. Where the government can limit the scope of the warrant in this manner, it must do so. *See United States v. George*, 975 F.2d 72, 76 (2d Cir. 1992) (The Fourth Amendment requires the government to identify the places to be searched and items to be seized with "as much particularity as the circumstances reasonably allow."). Indeed, some courts now require that warrants for provider-assisted searches contain restrictions such as data ranges. *See, e.g., In the Matter of a Warrant for All Content and Other Information Associated with the Email Account xxxxxx gmail.com*, 33 F. Supp. 3d 386, 394 (S.D.N.Y. 2014); *In re: [REDACTED]@gmail.com*, No. 14-70655-PSG, at 6 (N.D. Cal. 2014) (order denying application for a search warrant).

B. The Fourth Amendment May Require that the Government Observe Additional Privacy Safeguards When Directing a Provider to Assist in a Search of User Content.

In general, a provider assisting in a search as directed by a warrant identifies and produces to the government responsive documents or files. Unlike a government seizure of storage media during a physical search, the government need not search a user-created data environment or analyze forensic evidence of user activity. This has several implications.

First, reviewing documents produced by the provider does not require scarce forensic expertise. The case agent or another member of the investigative team can review the documents to identify responsive data and need not wait for a government forensic expert to do so.

Second, although a provider-assisted search may result in a large volume of documents, the government's review will entail merely looking at the documents produced by the provider and applying the criteria set forth in the warrant to identify the items within the production that the government may seize (a process similar to reviewing a box of physical documents). Reviewing documents produced by a provider does not require the technical and specialized forensic analysis that may be required when an agent is trying to tease out information hidden on seized electronic storage media. The reasonable time period within

which the Fourth Amendment requires the government to review the documents and files seized pursuant to a warrant should therefore, on average, be significantly shorter in a provider-assisted search than in a search of physical storage media seized from a residence or premises.

Third, even if this Court were to credit the government's argument that destroying files determined to be outside the scope of the warrant "would compromise the remaining data . . . making it impossible to authenticate or use it in a criminal prosecution," *Ganias*, 755 F.3d at 139 (*citing* Appellee Br. At 34), that argument would not apply to evidence resulting from a provider-assisted search. As noted above, the evidence resulting from such searches consists of files or documents that a provider copies from the service and provides to the government. The evidence does not result from forensic investigation and analysis of an authentic user environment. Providers may (and routinely do) therefore authenticate the results of provider-assisted searches by providing written certifications of authenticity. *See* U.S. Department of Justice, Searching and Seizing Computers and Electronic Evidence in Criminal Investigations at 199-200 (2009). In the context of a provider-assisted search, it simply would not "compromise the remaining data" or "make it impossible to authenticate or use" as

evidence if the government deleted records it determined to be outside the scope of the warrant.

Finally, Congress has not been silent on the circumstances under which records and evidence regarding a customer's use of a communications service should remain available to the government. Section 2703(f) of the criminal code authorizes the government to require a provider to "take all necessary steps to preserve records and other evidence pending the issuance of a court order or other process." The government may require a provider to retain such records and evidence for a total of 180 days: 90 days pursuant to an initial request and an additional 90 days pursuant to an extension. *See* 18 U.S.C. § 2703(f)(2). Where the government has reason to believe that records and other evidence regarding a customer's use of a communications service are relevant to a criminal investigation, Congress has authorized the government to ensure the records and evidence remain available for 180 days. It would be incongruous to establish a rule pursuant to which the government could ensure that records and evidence that the government had determined were *not* relevant to a criminal investigation nonetheless remained available indefinitely.

There may very well be other ways in which application of the Fourth Amendment to a provider-assisted search differs from its application to a search

and seizure of documents stored on physical media seized from a residence or business. Accordingly, even if this Court holds that the government did not violate the Fourth Amendment in this case, Google respectfully requests that the Court limit its holding to data stored on physical media seized during a search of a property or premises. If, as the preceding discussion suggests, it is possible for courts to require and the government to observe greater protections for privacy in the execution of warrants for files and documents stored with online service providers, then that is what the Fourth Amendment requires.

CONCLUSION

For the foregoing reasons, Google respectfully submits that the en banc Court should limit its holding to the facts of this case, involving files and documents stored on physical storage media seized during the search of Defendant's office.

DATED: July 29, 2015

PERKINS COIE LLP

By:/s/ Todd M. Hinnen

Todd M. Hinnen
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101-3099
thinnen@perkinscoie.com

Attorney for Amicus Curiae
Google Inc.

CERTIFICATE OF COMPLIANCE

The undersigned counsel for *amicus* certifies that the foregoing brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because it contains 3,748 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word 2003 in 14-point Times New Roman font.

DATED: July 29, 2015

PERKINS COIE LLP

By:/s/ Todd M. Hinnen

Todd M. Hinnen
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101-3099
thinnen@perkinscoie.com

Attorney for Amicus Curiae
Google Inc.

CERTIFICATE OF SERVICE

When All Case Participants Are Registered for the Appellate CM/ECF System

I hereby certify that on this 29th day of July, 2015, a true and correct copy of the foregoing BRIEF OF AMICUS CURIAE Google Inc. was served on all counsel of record in this appeal via CM/ECF pursuant to Second Circuit Rule 25.1(h)(1)-(2).

DATED: July 29, 2015

PERKINS COIE LLP

By:/s/ Todd M. Hinnen

Todd M. HInnen
Thinnen@perkinscoie.com

Attorney for Amicus Curiae
Google Inc.