Redacted Public

United States District Court
For the Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

In re: [REDACTED]@gmail.com

Case No. 14 70655 PSG

ORDER DENYING APPLICATION FOR A SEARCH WARRANT

On most days, the undersigned joins the teeming masses of the Bay Area on Highway 101 or 280. Lengthy queues form at each exit in Mountain View, Sunnyvale and Cupertino. Double decker buses pulse with their Wi-Fi as they move past in the diamond lane. On other days, on the ride to the courthouse on Caltrain, passenger after passenger bears the access badges that similarly mark the proliferation of the technology worker. A similar scene plays out as much at the humble downtown San Jose taqueria as the overpriced Palo Alto cafe. The Technorati are, in short, everywhere. And yet too few understand, or even suspect, the essential role played by many of these workers and their employers in facilitating most government access to private citizen's data.

Search warrant applications like the one presently before the court bring this role into view.

The tools of modern crime have evolved beyond a ski mask and a burlap sack. Like the rest of society, the modern criminal uses computers and mobile devices to do his "work." As such, evidence of crime and evidence of daily life unrelated to crime are often intertwined in software files, folders and databases. Even with a warrant issued under Fed. R. Crim. P. 41, this often leaves the government in the unenviable position of having to spend many, many hours of sifting through data by brute force or complex and cumbersome sorting algorithms. Where the computers at issue are at a suspect's home, courts have recognized the impracticality of reviewing the data on site by approving a "seize first, search second" methodology.[1]

But what about those computers that are not at a suspect's home, but at a third-party cloud provider like Google? Following a standard format used by the Department of Justice, the government draws no distinction and commonly seeks approval for the same seize first, search second methodology whether the data of interest is local or remote. For example, the supporting affidavit here is divided into three sections in which the first section gives background and the reasons sufficient to establish probable cause. In a second section, labeled "Attachment A," the property to be searched is identified as a particular email account stored on the premises of Google's headquarters. No date restriction is included. The third section, labeled "Attachment B," includes two subsections. Subsection I describes particular information within the account to be

[1] *See United States v. Hill*, 459 F.3d 966, 974-75 (9th Cir. 2005) ("[T]he process of searching the files at the scene can take a long time. To be certain that the medium in question does not contain any seizable material, the officers would have to examine every one of what may be thousands of files on a disk-a process that could take many hours and perhaps days. Taking that much time to conduct the search would not only impose a significant and unjustified burden on police resources, it would also make the search more intrusive. Police would have to be present on the suspect's premises while the search was in progress, and this would necessarily interfere with the suspect's access to his home or business. If the search took hours or days, the intrusion would continue for that entire period, compromising the Fourth Amendment value of making police searches as brief and non-intrusive as possible."); *see also United States v. Giberson*, 527 F.3d 882, 887 (9th Cir. 2008) ("[W]here there was ample evidence that the documents authorized in the warrant could be found on a person's computer, the officers did not exceed the scope of the warrant when they seized the computer.").

comes from the government. No defendant or defense counsel is present. Indeed, no defendant yet exists, as no case has yet been filed. There are no hearings, no witnesses, no briefs and no debate. Instead, a magistrate judge is left to predict what would or would not be reasonable in executing the warrant without any hard, ripe facts. This is hardly a recipe for success.[5]

And yet, despite Rule 41(d)(1)'s mandatory language,[6] this court must respect that this Circuit, the Ninth Circuit, has explicitly approved ex ante restrictions in search warrants. In particular, in *United States v. Hill*, the court mandated that agents looking to seize and then search must secure a magistrate judge's approval of the reasonableness of the approach in advance:

> Although computer technology may in theory justify blanket seizures for the reasons discussed above, the government must still demonstrate to the magistrate factually why such a broad search and seizure authority is reasonable in the case at hand. There may well be situations where the government has no basis for believing that a computer search would involve the kind of technological problems that would make an immediate onsite search and selective removal of relevant evidence impracticable. Thus, there must be some threshold showing before the government may "seize the haystack to look for the needle."[7]

And so this court must fulfill its duty to consider whether the restrictions of Attachment B pass muster.

This brings the court to the second element worthy of discussion: the constitutionality of the warrant application. As an initial matter, in many ways, the application is remarkably unremarkable. As it does on most days in this court, the government seeks data in the files of an electronic communications service provider as part of an ongoing investigation. Because this same type of request is regularly made in this district, the particular details of the investigation at issue

[5] *See Warshak v. United States*, 532 F.3d 521, 528 (6th Cir. 2008) ("The Fourth Amendment is designed to account for an unpredictable and limitless range of factual circumstances, and accordingly it generally should be applied after those circumstances unfold, not before."); *see also* Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV.1241, 1278-84 (2010).

[6] "[A] magistrate . . . must issue the warrant if there is probable cause."

[7] 459 F.3d 966, 975 (9th Cir. 2006).

here are not important for purposes of this discussion. Suffice it to say that the court finds probable cause to believe that the Gmail account at issue holds evidence of the theft of government funds.

But what of all the data associated with the account which supplies no such evidence whatsoever? In the Ninth Circuit anyway, the problem is not with seize first, search second itself. To understand why, go back to *Hill*. *Hill* was undeniably not a third-party provider case; Mr. Hill possessed all the hardware at issue. But in evaluating the warrant authorizing the seizure and search of Hill's computers, the Ninth Circuit weighed burdens and practical considerations that, if anything, are more compelling in a cloud computing environment, not less. Take, for example, the court's concern with facilitating technical accuracy in searching for the data of interest. In the absence of a seize first, search second approach, presumably Google (or a special master retained by Google) would have to search the account at issue looking for just the evidence to be seized. But even with its search prowess, Google would be left to guess what search terms would be appropriate. Would it be enough to look for "theft" within five words of "government funds"? Can Google rely on its famous search engine, or is human review required? Is it reasonable to impose the cost and, equally important, the distraction of such efforts on a third party to the investigation, especially in light of the number of times a company like Google gets such a request every month?

Alternatively, consider *Hill*'s concern with the burden on the suspect. Is the suspect better off with a private firm like Google so intimately involved in a live criminal investigation—or worse? While Google has publicly declared that it challenges overbroad warrants, in three-plus years on the bench in the federal courthouse serving its headquarters, the undersigned has yet to see any such motion. In addition, while not a Ninth Circuit decision, in *United States v. Bach*,[8] the

[8] 310 F.3d 1063, 1066-67 (8th Cir. 2002).

Eighth Circuit held that the Fourth Amendment permitted essentially the same two-step performed by Yahoo! at the behest of government investigators. Other district courts have similarly so held.[9]

The court is nevertheless unpersuaded that the particular seize first, search second proposed here is reasonable in the Fourth Amendment sense of the word. On past occasions, the government at least submitted a date restriction. Here, there is no date restriction of any kind. The activity described in the application began in 2010; Gmail has been broadly available since 2007 and in beta release since 2004. Nor has the government made any kind of commitment to return or destroy evidence that is not relevant to its investigation.[10] This unrestricted right to retain and use every bit Google coughs up undermines the entire effort the application otherwise makes to limit the obvious impact under the plain view doctrine of providing such unfettered government access.

A final point. This is not the first time that the substance of this application has been before a magistrate judge. On March 26, 2014, United States Magistrate Judge John Facciola denied a previous application for a similar warrant in the United States District Court for the District of Columbia. In his order Judge Facciola cited the "reasons stated in *In re Matter of the Search of Information Associated with [REDACTED]@Mac.com That is Stored at Premises Controlled by Apple, Inc.*, Mag. Case No. 14-228, 2014 WL 945563 (D.D.C. Mar. 7, 2014)." To the government's credit, it did not in any way hide its previous unsuccessful effort; in fact it both provided the disclosure in the sworn affidavit itself and attached a copy of the opinion to the application materials. And nothing in Rule 41 specifically prohibits this type of follow-up request in a second district after denial of an application in the first. But there is a long-recognized

[9] *See, e.g., United States v. Taylor*, 764 F. Supp. 2d 230, 237 (D. Me. 2011); *United States v. Bickle*, Case No. 10-cr-00565, 2011 WL 3798225, at *20 (D.Nev. Jul. 21, 2011); *United States v. Bowen*, 689 F. Supp. 2d 675, 682 (S.D.N.Y. 2010).

[10] *Cf. In the Matter of the Search of Information Associated with [Redacted] That is Stored at Premises Controlled by Yahoo! Inc.*, 13 M.J. 728, [#4] (D.D.C. Sept. 25, 2013) (sealed) (Facciola, M.J.).

United States District Court
For the Northern District of California

presumption against duplicating court efforts—what some charitably call judge shopping.[11] Even if a denial of an application were non-appealable, [12] the obvious alternative recourse available to the government was to seek a writ of mandamus under the All Writs Act or to return to Judge Facciola with a modified request. Under such circumstances, it would appear that what the government has chosen to do instead is nothing less than come west looking for a better result.

The application is DENIED. The clerk shall file a redacted copy of this order on the public docket but seal the search warrant, all documents related to search warrant and an unredacted copy of this order.

IT IS SO ORDERED.

Dated: May 8, 2014

PAUL S. GREWAL
United States Magistrate Judge

[11] *See, e.g., United States v. Leon*, 468 U.S. 897, 918 (1984); *United States v. Richardson*, 943 F.2d 547,551 (5th Cir. 1991); *United States v. Karathanos*, 531 F.2d 26, 34 (2d Cir. 1976).

[12] *See, e.g. United States v. Savides*, 658 F. Supp. 1399, 1404 (N.D. Ill. 1987), aff'd sub nom. *United States v. Pace*, 898 F.2d 1218 (7th Cir. 1990); *but see In re Historical Cellsite Data*, 724 F.3d 600, 605 (5th Cir. 2013) (collecting cases).