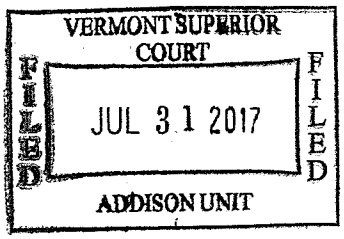
STATE OF VERMONT

SUPERIOR COURT CRIMINAL DIVISION
Addison Unit

In re Search Warrant in Case No. 16-MB-004413 (Addison Unit)

In re Search Warrant in Case No. 17AG000003 (Chittenden Unit)

In re Search Warrant in Case No. 15AG000082 (Washington Unit)



In these matters, consolidated in this unit for purposes only of hearing and decision on the common issue presented, the State of Vermont seeks to compel Google, Inc. to comply with search warrants commanding the production of electronic communications sent from or received by, and stored in Google customer accounts. The common issue involves the extent to which a Vermont court can require Google to produce information stored on servers located outside the United States. In each case, the affidavit supporting the warrant application established probable cause to believe that the account had been used by an individual located in Vermont to send, receive, or store evidence of criminal activity that occurred in Vermont; in fact, in each case, the affidavit established probable cause to believe that the sending, receipt, or storage of the communications at issue is itself criminal activity. The warrants all command Google to produce the relevant data sets to law enforcement in Vermont, there to be reviewed for actual evidence of such criminal activity described in the underlying affidavits. For the reasons set forth below, the court concludes that the warrants were proper, and so orders Google to produce the requested communications.

Background

At the outset, it bears noting that only the Washington Unit warrant presents a live controversy. In the Addison and Chittenden cases, Google has certified that all communications requested have been located on U.S. servers, and so have been produced. These cases, therefore, may be moot. Nevertheless, the parties appear to agree that the issues presented here may be sufficiently capable of repetition, yet avoiding meaningful review that the mootness doctrine would not compel dismissal. The court need not reach this question, however, as (at least at the

time of argument) there remain communications covered by the Washington Unit warrant stored on servers located outside the United States, as to which Google stands on its objection under the Stored Communications Act, 18 U.S.C. §§ 2701-12 ("SCA"). That case sufficiently presents the issues raised by the other two cases that the court need not wade into mootness waters. The court therefore confines its analysis to the facts and arguments presented in the Washington Unit case, confident that the answers found there will apply in all analogous cases.

The parties have stipulated to many of the facts necessary to the court's consideration of this question. Other facts are amply established, for the purposes of these motions, by the affidavit submitted in support of the search warrant application. Together, these materials establish that the communications that are the subject of the warrants here at issue were all sent or received by individuals amply shown to have been in Vermont when they sent, received, or stored the communications. The communications themselves have been amply shown to be likely to contain evidence of crimes committed in Vermont. All such communications are stored on Google accounts.

Google Inc. ("Google") is a U.S.-headquartered company incorporated in Delaware with a principal place of business in California. Among other things, Google offers users a variety of different online and communications services, including but not limited to its search engine, Gmail, Photos, and Google Drive services. Google provides these services to users around the world, including to individuals in Vermont.

Google stores user data in data centers in various locations, some of which are inside the United States and some of which are in countries outside the United States. Some user files may also be broken into component parts, and different parts of a single file may be stored in different locations (and, accordingly, different countries) at the same time. As far as appears from the stipulated facts, any relationship between the location of the user and the location(s) where that user's files are stored is coincidental. Google operates a state-of-the-art intelligent network that, with respect to some types of data including some of the data at issue in this case, automatically moves data from one location on Google's network to another as frequently as needed to optimize for performance, reliability, and other efficiencies. As a result, the country or countries in which specific user data, or components of that data, are located may change. It is therefore possible, for example, that the network will change the location of data between the time when legal process is sought by law enforcement and when it is served on Google. As another

example, it is equally possible that after Google responds to a search warrant, data that were located in another country at the time of the production will move into the United States. In addition, for certain types of data, including some of the data at issue in this case, Google's tool that queries the network does not report the country in which foreign-stored data is located.

Law enforcement officers may submit search warrants to Google electronically from anywhere in the world, including from Vermont. Google can produce its responses electronically. Law enforcement may retrieve Google's responses from anywhere in the world, including from Vermont. In the above-captioned matters, law enforcement retrieved and is reviewing Google's responses to the warrants referenced in the attached Exhibit List, all while located in Vermont.

Only personnel in Google's Legal Investigations Support team are authorized to access the content of communications in order to produce it in response to legal process. All such Google personnel are located in the United States. At argument, Google's counsel conceded that a Google employee with the requisite knowledge and clearance could retrieve the data sought by these warrants from any computer, anywhere—even the court's own computer, on the bench.

Analysis

The warrant in the Washington Unit case—indeed, in all of these cases—issued pursuant to the Vermont Electronic Communication Privacy Act, 13 V.S.A. §§ 8101-08 ("VTECPA"), following the procedure set forth in V.R.Cr.P. 41. By its express terms, VTECPA contains no territorial limitations. Rather, it allows a Vermont court to issue warrants to search and seize electronic communications without reference to the location where they may be stored, as long as the warrant is served on a service provider with sufficient minimum contacts with Vermont to establish personal jurisdiction. *See* 13 V.S.A. § 8107(a). The parties appear to agree that Google fits this description, and further that a warrant issued pursuant to VTECPA properly reaches communications stored anywhere in the United States. They disagree, however, whether such a warrant may properly reach communications stored outside the United States.

The parties have focused their rhetorical efforts on the SCA and the burgeoning body of federal caselaw interpreting that statute in contexts similar to that presented here. The lightning rod in these debates has been the Second Circuit's treatment of the issue in *Microsoft Corporation v. United States*, 829 F.3d 197 (2d Cir. 2016) ("*Microsoft I*"), and *Microsoft*

Corporation v. United States, 855 F.3d 53 (2d Cir. 2017) ("*Microsoft II*"). In the first of those decisions, the Second Circuit held first that the SCA does not authorize extraterritorial warrants, and second that warrants issued pursuant to the SCA therefore could not properly compel the production of data stored outside the United States. *See Microsoft I*, 829 F.3d at 216, 220-21. In the second, an even split among the remaining judges on the court resulted in the denial of rehearing *en banc*. *Microsoft* II, 855 F.3d at 54. Virtually every decision cited by the parties uses one or both of the *Microsoft* decisions as its jumping-off point. As the most recent of these decisions points out, "[e]very court outside the Second Circuit that has considered the issue has rejected the holding of *Microsoft* and has concluded that the disclosure of electronic information accessed within the United States but stored on servers abroad does not implicate extraterritoriality concerns." *In the Matter of the Search of Info. Associated with [Redacted]@gmail.com That Is Stored at Premises Controlled by Google, Inc*, 2017 WL 2480752, at *6 (D.D.C. June 2, 2017) (collecting cases).

This court need not jump directly into the *Microsoft* debate, however, for one very important reason. All of the courts in those cases were called upon to determine the permissible scope of a federal warrant issued under the authority of the SCA, and pursuant to the Federal Rules of Criminal Procedure. In the cases before this court, in contrast, the warrants were issued under the authority of VTECPA, and pursuant to the Vermont Rules of Criminal Procedure. The SCA does not purport to regulate state warrant procedure; it requires only that any stored communications be released only pursuant to a warrant issued by a "court of competent jurisdiction" using (in the case of a state court) "State warrant procedures." 18 U.S.C. § 2703(a) & (b)(1)(A). The SCA defines "court of competent jurisdiction" as including "a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants." 18 U.S.C. § 2711(3)(B). This court is plainly such a court. Whether this court had proper authority to issue these warrants is beyond the purview of the SCA—except to the extent that the SCA might be construed as either narrowing or broadening such authority. That it plainly does not do. Thus, the SCA's only relevance in the cases at bar lies in its recognizing a privacy interest (and, hence, a warrant requirement) where none might otherwise exist. *See In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 145 (3d Cir. 2015) ("the Stored Communications Act was born from congressional recognition that neither existing federal statutes nor the Fourth Amendment protected against potential intrusions on individual privacy

arising from illicit access to stored communications in remote computing operations and large data banks that stored e-mails" (internal quotation marks omitted)); *Microsoft I*, 829 F.3d at 206 ("As the government has acknowledged in this litigation, '[t]he SCA was enacted to extend to electronic records privacy protections analogous to those provided by the Fourth Amendment.' " (brackets in original)).

Google does not argue that VTECPA contains a territorial limitation. Indeed, in acknowledging that the warrants in this case properly compel production of communications stored anywhere in the United States, Google appears to concede that a VTECPA warrant may properly reach data stored beyond state borders.[1] Google provides no authority, nor even makes any argument to support the proposition that while a VTECPA warrant may properly reach data stored, for example, across Lake Champlain, it may not reach data stored across the Atlantic. Instead, Google argues that the permissible scope of any warrant for stored communications is constrained by the SCA. But the SCA plainly neither expands nor constricts the authority of a Vermont court. Again, all the SCA requires is that state warrants be issued using state warrant procedures.

Nothing in Vermont Rule of Criminal Procedure 41 purports to limit the territorial scope of a warrant. Equally, VTECPA does not so limit the scope of a warrant; all it requires is that the communications sought be in the possession of an individual or entity subject to personal jurisdiction in the state. *See* 13 V.S.A. § 8107(a). The question, then, is whether there is some organic limitation, inherent in the requirement of a warrant.

The answer, acknowledged at argument by both parties, is that there is such a limitation. The limitation inheres in our constitutional structure, informed by concepts of international law and comity. *See, e.g.*, Restatement (Third) of Foreign Relations Law in the United States

---

[1] Reduced to its bare essentials, Google's argument rests on the major premise that a court lacks jurisdiction to issue a warrant with extraterritorial effect. This assertion is uncontroversial. Google's suggested conclusion, however, rests on a separate, minor premise: that a warrant that requires the production of data stored beyond a state's boundaries has extraterritorial effect. As the *Microsoft* debate illustrates, this premise is far more controversial.

In this regard, the court notes that Google advertises on its website that it has data storage centers in seven states. *Data Center Locations*, google.com, https://www.google.com/about/datacenters/inside/locations/index.html (last visited July 28, 2017). Research reveals that not all of these states have reciprocity provisions analogous to that found in the VTECPA. *See* 13 V.S.A. § 8107(c). The only way a VTECPA warrant could properly reach data stored in one of the states lacking a reciprocity provision is if the court had organic authority to compel the production of data stored outside state limits. In conceding that a VTECPA warrant may properly reach communications stored in these states, Google has effectively admitted that the court has such authority, and so refuted its own minor premise.

§ 432(2) (1987) ("A state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state."); *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286, 293 (1980) ("The sovereignty of each State, in turn, implied a limitation on the sovereignty of all of its sister States—a limitation express or implicit in both the original scheme of the Constitution and the Fourteenth Amendment."). In short, a state's authority —and hence its judiciary's—has territorial limits. *See, e.g., Townsend v. Jemison*, 50 U.S. 407, 416 (1850) ("the obligation of every law is confined to the State in which it is established, [and] it can only attach upon those who are its subjects, and upon others who are within the territorial jurisdiction of the State"); *McDonald v. Mabee*, 243 U.S. 90, 91 (1917) ("[t]he foundation of jurisdiction is physical power").

To this extent, then, the *Microsoft* debate, while in no way controlling, may at least be instructive. In *Microsoft I*, the court concluded that a warrant requiring the production of data stored in a server in Ireland was not permitted by the SCA. The court noted that "[w]arrants traditionally carry territorial limitations," 829 F.3d at 201, and concluded that the warrant in question violated these limitations, *id.* at 222. Its conclusion was itself conclusory:

> Although the Act's focus on the customer's privacy might suggest that the customer's actual location or citizenship would be important to the extraterritoriality analysis, it is our view that the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed—here, where it is seized by Microsoft, acting as an agent of the government. Because the content subject to the Warrant is located in, and would be seized from, the Dublin datacenter, the conduct that falls within the focus of the SCA would occur outside the United States, regardless of the customer's location and regardless of Microsoft's home in the United States.

Id. at 220.

There are multiple flaws with this "analysis," amply exposed in the many opinions since *Microsoft I* that have reasoned to the opposite result. *See, e.g., Microsoft II*, 855 F.3d at 60-76 (Jacobs, Cabranes, Raggi, and Droney, JJ., dissenting); *In re Search Warrant to Google, Inc.*, 2017 WL 2985391, at *9-11 (D.N.J. July 10, 2017); *Search of Info. Associated with [Redacted]@gmail.com*, 2017 WL 2480752, at *6-11. In one respect, however, the *Microsoft I* majority got it right. The focus of the warrant requirement is government action. *See U.S. v. Jacobsen*, 466 U.S. 109, 113 (1984) (the "Court has also consistently construed [Fourth Amendment] protection as proscribing only governmental action"). The *Microsoft I* majority

found government action when "Microsoft, acting as an agent of the government," seized data located in Ireland. *Microsoft I*, 829 F.3d at 220. Google, however, does not argue here that it acts as an agent of the government when it reaggregates data that is already in its possession, wherever stored. Indeed, in the most recently-decided SCA case cited by the parties, Google "insist[ed] that it does not act as an agent of the government when it accesses its user's data pursuant to an SCA warrant." *Search of Info. Associated with [Redacted]@gmail.com*, 2017 WL 2480752, at *10. As that court noted, this "concession is also well taken. A service provider is not properly viewed as acting as an agent of the government when 'seizing'—or, more appropriately, simply accessing—customer content pursuant to an SCA warrant." *Id.*; *see also Microsoft* II, 855 F.3d at 72 (Raggi, J., dissenting) ("I cannot agree that a person who is compelled by a § 2703(a) warrant to disclose to the government materials already in that person's possession is 'seiz[ing]' anything as an agent of the government." (brackets in original)). Leaving aside the question of what constitutes "seizure" of something as ephemeral as the data at issue in these cases,[2] this observation renders the *Microsoft I* analysis completely useless in this case—except to the extent that it proceeds from the uncontroversial precept that warrants have territorial limits. Again, however, the critical point is that the limit is on *government* action.

As the *Microsoft I* majority recognized, "the focus of the SCA's warrant provisions is on protecting users' privacy interests in stored communications." 829 F. 3d at 220. That focus is not limited to the SCA; it is inherent in any warrant requirement. In each instance, the requirement serves to protect privacy interests against unreasonable government intrusions. *See Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 621–22 (1989) ("An essential purpose of a warrant requirement is to protect privacy interests by assuring citizens subject to a search or seizure that such intrusions are not the random or arbitrary acts of government agents."). The territorial limit on a court's—or a state's—jurisdiction is one facet of that protection. The question is which state can act in derogation of recognized privacy interests, and so which court must review that action to be sure it is not unreasonable.

---

[2] Multiple authorities have argued persuasively that there is no "seizure" when all the government acquires is a copy—whether of a photograph, document, or dataset—because the owner's possession of the original remains undisturbed. *See, e.g., Search Warrant to Google, Inc.*, 2017 WL 2985391, at *11; *Search of Info. Associated with [Redacted]@gmail.com*, 2017 WL 2480752, at *10; *In re Search Warrant No. 16-960-M-01 to Google*, 2017 WL 471564, at *10 (listing cases). The SCA and VTECPA have mooted this question, at least in the present context, in requiring a warrant whenever the government seeks to compel production of electronically stored communications.

Google would argue that this analysis must be undertaken in every location where any electronic communication is stored, in whole or in part. As noted above, however, Google does not argue in this case that its retrieval of such data constitutes state action, and very recently it has asserted that its retrieval is not state action. *Search of Info. Associated with [Redacted]@gmail.com*, 2017 WL 2480752, at *10. Rather, state action occurs in these cases when the State of Vermont, with warrant in hand, compels Google, which is subject to the State's jurisdiction, to produce in Vermont data in Google's possession, wherever located. The State searches no premises—inside Vermont or elsewhere. Rather, the only "search" occurs in Vermont, when the State reviews the dataset produced by Google. Equally, the only "seizures" occur in Vermont, first when the State receives the dataset produced by Google, and then when it extracts from that dataset any communications that may be evidence of a crime. It is only in Vermont that the State acts in any way to implicate the privacy interests of the owner(s) of the data at issue. *Cf. Microsoft I*, 829 F.3d at 220 ("it is our view that the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed"). It follows that this is where those interests should be protected.

In this regard, then, a VTECPA warrant functions much as an investigative subpoena. It is by no means an extraordinary assertion of the State's sovereignty. In multiple contexts, the State has asserted the right to compel those subject to its personal jurisdiction to produce materials in their possession, without respect to location. *See, e.g.,* V.R.C.P. 34(a) (requiring party to civil suit to produce "any tangible things . . . in the possession, custody or control of the party"); V.R.C.P. 45(a)(1)(C) (authorizing subpoena served within the state to "command each person to whom it is directed . . . to produce . . . things in the possession, custody or control of that person"); V.R.Cr.P. 17(c) ("subpoena may . . .command the witness . . .to produce the books, papers, documents or other objects designated therein"); 8 V.S.A. § 13(a) (authorizing Commissioner of Financial Regulation to "require production of papers and records"); 9 V.S.A. § 5602 (authorizing Commissioner of Financial Regulation to "require the production of any records . . . relevant or material to [a securities investigation]"); 11 V.S.A. § 441(a) (requiring corporation doing business within the state to produce on notice "all books, documents, correspondence, memoranda, papers, and data . . . which have been made or kept at any time within this State, and are in the custody or control of the corporation in this State or elsewhere at the time of service of the notice upon it."). The court has searched in vain for a single instance in

which the State's authority in this regard has been questioned, much less limited, on territorial grounds. As long as the person commanded to produce materials is subject to the State's *in personam* jurisdiction, the authority to command such production is unquestioned. *Cf.* 9A Charles Alan Wright and Arthur R. Miller, Federal Practice and Procedure, § 2456 n.5 (3d ed.) ("The case law clearly has established that even records kept beyond the territorial jurisdiction of the district court issuing the subpoena may be covered if they are controlled by someone subject to the court's jurisdiction.").

The examples above are all garden-variety illustrations of a fundamental attribute of a state's sovereignty: the authority to compel certain acts by individuals or entities subject to the state's jurisdiction. The difference among the various assertions of this authority lies principally in the means by which it is exercised, affecting in turn the manner and timing of any judicial review to protect the rights of the individuals or entities involved. In the case of warrants, that review is mandatory, occurs before the issuance of process, and includes rigorous substantive and procedural protections; in the case of notices to produce and subpoenas, review generally occurs at the request of a party, after the issuance of process, and is somewhat narrower.

For the purposes of these cases, then, the principal function of the SCA and VTECPA is to prescribe the manner in which the State's unquestioned authority must be exercised. To read the warrant requirement as requiring anything more than that—as somehow divesting the state of authority over persons or entities subject to its personal jurisdiction—reads far more into these statutes than either the principles of statutory interpretation or common sense allow. Thus, as observed by one of the *Microsoft II* dissenters, "[i]t is simply unprecedented to conclude that the presumption against extraterritoriality bars United States courts with personal jurisdiction over a United States person from ordering that person to produce property in his possession (wherever located) when the government has made a probable cause showing that the property is evidence of a crime." 855 F.3d at 70 (Raggi, J., dissenting).

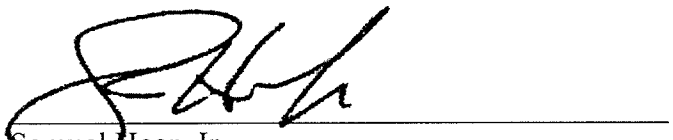
There is no suggestion here that this court lacks personal jurisdiction over Google. Equally, there is no suggestion that Google does not have the data sought in its possession. There is no suggestion that the court lacked probable cause to issue the warrants at issue, or that the procedure employed in the issuance of the warrants was somehow defective. In short, there is no basis for arguing that these warrants were not issued by a court of competent jurisdiction using state warrant procedures. Rather, VTECPA and V.R.Cr.P. 41 clearly authorize the issuance of

these warrants, and the SCA does not constrain that authority. The warrants, therefore, must be enforced.

ORDER

The Motion to Compel is **granted**. Google is ordered to produce all data described in the Washington Unit warrant, wherever located. The parties having represented that Google has fully complied with the Addison and Chittenden Unit warrants, no order issues with respect to those warrants.

Electronically signed on July 31, 2017 at 12:26 PM pursuant to V.R.E.F. 7(d).



Samuel Hoar, Jr.
Superior Court Judge