UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

San Francisco Division

UBER TECHNOLOGIES, INC.,

Plaintiff,

v.

JOHN DOE I,

Defendant.

Case No. 15-cv-00908-LB

ORDER GRANTING EXPEDITED-DISCOVERY & RELATED SEALING MOTIONS

[Re: ECF Nos. 16-19]

INTRODUCTION

Plaintiff Uber Technologies, Inc. claims that defendant John Doe I breached its secure database, stole information from that database, and so violated the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030 et seq., and the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502. (Compl. – ECF No. 1 at 2, ¶ 8.)[1] In its continued effort to identify Doe, Uber seeks permission to take expedited discovery from third parties Comcast Business Communications, LLC (ECF No. 16) and GitHub, Inc. (ECF No. 18). Uber seeks to discover (among other things) the names, physical addresses, email addresses, subscription-payment information, and Media Access Control addresses associated with identified Internet Protocol ("IP") addresses and a domain name that were likely used to access Uber's database.

[1] Record citations are to documents in the Electronic Case File ("ECF"); pinpoint citations are to the ECF-generated page numbers at the tops of the documents.

(The full subpoenas appear at ECF No. 16-1 at 7 and ECF No. 18-1 at 7.) Uber also brings two sealing motions, one related to each discovery motion, to maintain the confidentiality of the IP addresses and the domain name in the subpoenas — the disclosure of which (according to Uber) could help Doe elude its investigation. Finally, Uber asks the court to clarify its previous order (ECF No. 11) to confirm that Uber may "share information received in discovery in this lawsuit" with "third parties such as law enforcement" if such sharing is "in connection with Uber's claims in this lawsuit." (ECF No. 18 at 7.) For the reasons given and subject to the conditions set out below, the court grants all four of Uber's motions.

DISCUSSION

The court previously granted Uber's motion to take expedited discovery from GitHub. (ECF No. 11.) Uber's present motions walk mostly the same ground as its first motion and, insofar as they apply, the court incorporates by reference the factual and legal discussions in its previous order. As the court there found, Uber has shown that: (1) John Doe I is a real person who may be sued in federal court; (2) Uber unsuccessfully tried to identify John Doe I before filing these motions; (3) its claims against John Doe I could withstand a motion to dismiss; and (4) there is a reasonable likelihood that the proposed subpoenas will lead to information identifying John Doe I. The court extends its earlier factual discussion and legal analysis as needed to account for Comcast (who was not involved in the earlier motion) and for events following the issuance of Uber's first subpoena.

I. ECF NO. 16 — COMCAST

GitHub produced information in response to Uber's earlier subpoena. (Snell Decl. – ECF No. 16- 1 at 2, ¶ 3.) That information showed that "someone used an IP address registered to Comcast to access relevant posts on the GitHub site." (See id. at 2, ¶ 4; ECF No. 16 at 3, 5.) (The same person who breached Uber's database accessed the GitHub posts to which Uber refers. (ECF No. 4-2 at 1-2, ¶¶ 2-3.)) It is likely that Comcast "has subscriber information for the Address, as well as information potentially linking the subscriber to unauthorized access to Uber systems." (ECF No. 16 at 5.) "Thus," Uber writes, "information related to" the Comcast IP address "will further

Uber's investigation regarding the identity of John Doe 1." (Id. at 3.) The subpoena that Uber would now serve accordingly asks Comcast to produce:

> 1. The name, address, telephone number, email address, Media Access Control addresses, and any other identifying information for each subscriber assigned the Internet Protocol address [REDACTED] ("Subscribers") from March 11, 2014 until May 13, 2014.
>
> 2. Any logs or other information regarding Subscribers' access to the following IP addresses or domains between March 11, 2014 and May 13, 2014: (a) [REDACTED]; and (b) [REDACTED].
>
> 3. Any logs or other information regarding Subscribers' access to the following IP addresses or domains on May 12, 2014 on or about 9:47 pm PDT: (a) [REDACTED]; and (b) [REDACTED].
>
> 4. The name, address, telephone number, email address, Media Access Control address, and any other identifying information for any individual user or machine on Subscribers' networks that accessed
>
> https://gist.githubusercontent.com/hhlin/9556255/raw/2a4fae0e6d443b29826096fe043409e2c305bb79/insurance fun.py, https://api.github.com/gists/9556255/, and/or https://gist.github.com/hhlin/9556255 on or about April 12, 2014.
>
> 5. The Subscribers' means and source of payment (including any credit card or bank account number).

(ECF No. 17-3 at 1.)

Producing this information should not unduly prejudice Comcast. Comcast is a sophisticated business that is likely accustomed to responding to subpoenas so that, as Uber contends, it "will not be burdened by this straightforward request involving one IP address." (ECF No. 16 at 5.) More precisely, Uber's need for the requested discovery outweighs whatever small burden the subpoena may impose on Comcast. See Semitool, Inc. v. Tokyo Electron Am., Inc., 208 F.R.D. 273, 276 (N.D. Cal. 2002).

The court furthermore deems the requested — and now authorized — subpoena to be issued "pursuant to a court order" within the meaning of 47 U.S.C. § 551(c)(2)(B). The relevant part of that statute provides:

> (c) Disclosure of personally identifiable information
>
> . . . .

> (2) A cable operator may disclose such information if the disclosure is —
>
> . . . .
>
> (B) . . . made pursuant to a court order authorizing such disclosure, if the subscriber is notified of such order by the person to whom the order is directed.

47 U.S.C. § 551(c)(2)(B). This order expressly authorizes such disclosure. To ensure compliance with this statute, the concluding section of this order provides for Comcast to notify Doe of the subpoena.

II. ECF NO. 18 — GITHUB

A. The Subpoena

Uber seeks to serve a new subpoena on GitHub. It explains:

> The instant request differs from Uber's prior request to GitHub. The prior request sought information related to visits to GitHub webpages over the course of several months and could therefore involve individuals who have nothing to do with the instant dispute. This request, however, is narrowly tailored to seek identifying information for the individual who used the same Address on the GitHub website on the same day that John Doe I used the Address to access Uber's database. . . . [T]his information will likely tie an individual directly to the breach . . . .

For the reasons given in its earlier order (ECF No. 11 at 3-6), the court holds that Uber has shown good cause for issuing the requested subpoena.

B. GitHub Need Not Notify John Doe

Uber also asks that, unlike it did with the last GitHub subpoena, the court not direct Uber or (more accurately) GitHub to notify Doe of the subpoena. "[T]here is no notice requirement under the law or GitHub's Terms of Service," Uber reasons. (ECF No. 18 at 6.) The court accepts GitHub's representations about the absence of such a requirement in the law; the court, too, has seen no law affirmatively requiring, in this situation, that someone be notified when their information will be turned over to an adversary in litigation pursuant to a lawful subpoena. And Uber is correct about GitHub's Terms of Service. As Uber recounts, the Terms of Service to which John Doe I must have agreed when he set up a GitHub account provide that, "GitHub may disclose personally identifiable information under special circumstances, such as to comply with subpoenas or when your actions violate the Terms of Service." (See ECF No. 18 at 6.) Uber

appears to be equally correct when it writes: "By accessing the GitHub site, John Doe I consented to disclosure of his personal information in connection with an investigation into illegal activities." (Id.) GitHub's privacy policy states: "The information we collected . . . is not shared . . . except to provide products or services you've requested, when we have permission, or under the following circumstances: It is necessary to share information in order to investigate, prevent, or take action regarding illegal activities . . . ." (See id.)[2]

The case that Uber cites in this area — *Sony Music Entm't Inc. v. Does 1*-40, 326 F. Supp. 2d 556 (S.D.N.Y. 2004) — does suggest that, in view of their Internet service provider's ("ISP") Terms of Service, Doe defendants had a "minimal expectation of privacy." Id. at 566. (The ISP in Sony Music did notify the Doe defendants that their identifying information had been subpoenaed. Id. at 559-60. The case does not mention whether this was at a court's direction or not.) It is one thing, however, to agree that one's information might be shared; it is another to waive notification of that fact. Notice has its own value. Being told that one's personal information is being disclosed may prompt one to take perfectly legitimate actions in response, even if a prior agreement bars one from objecting to the disclosure itself.

Uber has pointed out that Internet-anonymity cases come in different shades. On one end of the spectrum, anonymous-speech cases can directly implicate the First Amendment. These elicit the most demanding justification for disclosing an otherwise anonymous person's identity. See generally, e.g., In re Anonymous Online Speakers, 661 F.3d 1168, 1174-77 (9th Cir. 2011). Somewhere in the middle are copyright-infringement suits. See, e.g., Pink Lotus Entm't, LLC v. Doe, 2012 WL 260441, *2- (E.D. Cal. Jan. 23, 2012) (discussing Ninth Circuit good-cause standard) ("Good cause for expedited discovery is frequently found in cases involving claims of infringement . . . ."). This case lies near the opposite end of the spectrum. Here, Uber alleges that Doe directly breached and stole data from its secure database. On Uber's apparent view, the defendant in such a case can have little or no expectation that he will be notified, to say nothing of having a legal right to be notified, if an investigation discloses his personally identifying

[2] https://help.github.com/articles/github-privacy-policy/ (last accessed Apr. 22, 2015).

information.

This line of argument prompts two thoughts. The first is that this sort of case (call it one of straightforward hacking and data theft) shares more in common with copyright-infringement suits than with true First Amendment, anonymous-speech cases.[3] Infringement suits, too, involve theft; and defendants in such cases almost certainly are tempted "to destroy or tamper with evidence" upon learning that an investigator (adversarial litigant or law enforcement) is about to learn their identity. Nor has the court seen anything suggesting that the evidence that Doe may possess here is more ephemeral than the proof that is normally involved in infringement cases of illegal downloading and sharing. Yet infringement decisions have required the notice that Uber asks the court to excuse. E.g., Digital Sin, Inc. v. Does 1-176, 279 F.R.D. 239, 244 (S.D.N.Y. 2012) (ordering ISP to notify Doe defendant of subpoena); Warner Bros. Record Inc. v. Does 1-14, 555 F. Supp. 2d 1, 2 (D.D.C. 2008) (ordering ISP to notify anonymous subscribers "within five business days" of being served with subpoena issued under 47 U.S.C. § 551(c)(2)(B)).

Second, even if no law affirmatively requires that Doe be given notice in a case like this, notice may still be the better, fairer practice. It has been this court's standard practice to require notice to parties whose information will be disclosed under a lawful subpoena, even where no law positively requires that; other courts appear to take the same approach. See AF Holdings, LLC v. Doe, 2012 WL 5464577, *4 (E.D. Cal. Nov. 7, 2012); Digital Sin, 279 F.R.D. at 244-45.

Having said all that, and weighing seriously Uber's situation and its sensible reasoning, the court holds that, in this case, GitHub need not notify Doe of the subpoena. This does not mean that notice will be excused in every similar case. The decision here is motivated in significant part by two related facts. First, Doe's alleged act was an unauthorized intrusion into a secure area; this cannot have been legitimate under any scenario — and is somewhat different from cases that involve the downloading and sharing of material that, at least in principle, can in the first instance be gotten legitimately. Second, Uber seems moved equally to redress crime as to seek recompense

[3] The court says "true" First Amendment cases because copyright-infringement defendants have occasionally claimed that their activity is constitutionally protected speech. See Sony Music, 326 F. Supp. 2d at 562-65.

through civil remedies. The statutes that it sues under are both criminal. (See Compl. – ECF No. 1 at 3.)[4] Furthermore, in its request to share the subpoenaed information with third parties (a request that is discussed below), Uber suggests that it may turn over the discovered information to law enforcement. (ECF No. 18 at 7.) Assuming that its allegations are accurate, then, Uber's lawsuit would benefit wider society as well as benefiting Uber. Finally, if Doe finds something improper in his not being prospectively notified of the disclosure, he will have his opportunity to make those arguments later in this case, and may challenge Uber's right to use the information gained through the subpoena.

B. Clarification & Information Sharing

"Uber also seeks clarification of the Court's prior Order to confirm that Uber may share information with third parties who may assist Uber in its investigation or in this matter, such as law enforcement, should Uber decide it appropriate to do so." (ECF No. 18 at 7.) The court's previous order stated that, "Uber may use the subpoenaed information only in connection with its instant claims under the federal Computer Fraud and Abuse Act, and the California Comprehensive Computer Data Access and Fraud Act." (ECF No. 11 at 7.)

The court agrees that it is consistent with the purposes of these statutes — both of which establish data breaches and theft as crimes — that Uber be allowed to turn over material information to law enforcement. To avoid any uncertainty, moreover, and though it is perhaps obvious, Uber may also share the subpoenaed information with third parties that are technically necessary to Uber's investigation. Like Uber itself, such adjutant third parties must otherwise keep the information confidential.

III. THE SEALING MOTIONS — ECF NOS. 17 AND 19

Finally, Uber moves to seal limited parts of the Comcast and GitHub subpoenas. (ECF Nos. 17, 19.) Uber would redact two IP addresses and one domain name from the Comcast subpoena (see ECF No. 16-1 at 7) and one IP address from the new GitHub subpoena (see ECF No. 19-4 at

[4] See 18 U.S.C. § 1030(c)(4) (establishing imprisonment for certain violations of Computer Fraud and Abuse Act); Cal. Penal Code §§ 502(c)-(d) (establishing computer-data theft as "public offense" subject to fines and imprisonment).

1). In both cases, Uber argues that these items constitute "sensitive information that, if publicly disclosed, could undermine Uber's investigation into the data theft at issue in this lawsuit." (ECF Nos. 17 at 2, 19 at 2.) Publicly disclosing the target IP addresses and domain name, Uber says, could "giv[e] John Doe I insight into the status of Uber's investigation and thus" enable him "to take steps to further conceal his identity." (Id.)

Because the material in question relates to a non-dispositive motion, Uber must show only that there is "good cause" to seal it. E.g., Pintos v. Pac. Creditors Ass'n, 565 F.3d 1106, 1116 (9th Cir. 2009) opinion amended and superseded on denial of reh'g, 605 F.3d 665 (9th Cir. 2010); Kamakana v. City & County of Honolulu, 447 F.3d 1172, 1179-80 (9th Cir. 2006). Largely for the reasons that Uber states (ECF Nos. 17 at 2-3, 19 at 2-3), the court holds that Uber has shown "good cause" for sealing the IP addresses and domain name. The court accepts Uber's assertion that revealing the information in question could prompt Doe to elude detection, and thus thwart Uber's case at the outset, before the court can assess the merits of Uber's claims. Equally important, sealing two IP addresses and one domain name will in no significant way diminish the public's ability to "keep a watchful eye on the workings of" the court. See Kamakana, 447 F.3d at 1178-80. Furthermore, Uber has "narrowly tailored" its redactions to remove from the public record a minimum of information and only such information as is properly "sealable." See Civ. L.R. 79-5(b); Dish Network, LLC, Sonicview USA, Inc., 2009 WL 2224596 (July 23, 2009) (sealing records in satellite-television-piracy case partly because revealing investigators' identities would "jeopardize the success of [the plaintiff's] investigations").

CONCLUSION

The court grants both Uber's sealing motions. The court grants Uber's motion to serve its proposed subpoena (see ECF No. 18-1 at 4-7 (redacted)) on GitHub. Neither Uber nor GitHub is required to give Doe notice of the subpoena or that GitHub is producing personally identifying information. The court grants Uber's motion to serve its proposed subpoena (see ECF No. 16-1 at 4-7 (redacted)) on Comcast. Under 47 U.S.C. § 551(c)(2)(B), and consistent with the court's usual practice, the Comcast subpoena (but not the GitHub subpoena) is subject to the following

directions:

1. Uber may immediately serve the proposed subpoena on GitHub. The subpoena shall have a copy of this order attached. To the extent that producing the information sought is burdensome, the parties must meet and confer and comply with the discovery procedures in the court's standing order.

2. GitHub will have five business days from the date that the subpoena is served upon it to serve John Doe I with a copy of the subpoena and a copy of this order. GitHub may serve John Doe I using any reasonable means, including written notice sent to his or her last known address, transmitted either by first-class mail or via overnight service.

3. John Doe I shall have 30 days from the date of service upon him or her to file any motions in this court contesting the subpoena (including a motion to quash or modify the subpoena). If that 30-day period lapses without John Doe I contesting the subpoena, GitHub shall have 10 days to produce the information responsive to the subpoena to Uber.

4. GitHub shall preserve any subpoenaed information pending the resolution of any timely motion to quash.

5. GitHub must confer with Uber and must not assess any charge in advance of providing the information requested in the subpoena. If GitHub elects to charge for the costs of production, it must provide a billing summary and cost reports that serve as a basis for such billing summary and any costs claimed by GitHub.

6. Uber may use the subpoenaed information only in connection with its instant claims under the federal Computer Fraud and Abuse Act, and the California Comprehensive Computer Data Access and Fraud Act — as that use has been clarified by this order.

This disposes of ECF Nos. 16, 17, 18, and 19.

IT IS SO ORDERED.

Dated: April 27, 2015

LAUREL BEELER
United States Magistrate Judge

United States District Court
Northern District of California