Bathaee :: Dunne :: LLP

FILED UNDER SEAL

May 31, 2023 **Via CM/ECF**

Re: *Klein v. Meta Platforms, Inc.*, No. 3:20-cv-08570-JD (N.D. Cal.)

Dear Judge Donato:

Advertiser Plaintiffs ("Advertisers") respectfully request that the Court find that a *prima facie* case exists under the crime-fraud exception with respect to certain communications currently being withheld by Defendant Meta Platforms, Inc. ("Facebook") as attorney-client privileged. The communications at issue relate to Facebook's so-called In-App Action Panel ("IAAP") program, which existed between June 2016 and approximately May 2019. The IAAP program, launched at the request of Mark Zuckerberg, used a cyberattack method called "SSL man-in-the-middle" to intercept and decrypt Snapchat's—and later YouTube's and Amazon's—SSL-protected analytics traffic to inform Facebook's competitive decisionmaking. As described below, Facebook's IAAP program conduct was not merely anticompetitive, but criminal—the program violated 18 U.S.C. § 2511(a) and (d), the so-called "Wiretap Act," with no applicable exception. Facebook's attorneys were pervasively involved in the design, execution, and expansion of this program. On May 15, 2023, Advertisers sent Facebook a nineteen-page single-spaced letter providing screenshots, quotations from documents, and evidentiary citations setting forth the company's applicable conduct; analyzing that conduct under 18 U.S.C. § 2511, *et seq.* and under the Ninth Circuit's crime-fraud test, *see In re Grand Jury Investigation*, 810 F.3d 1110, 1113 (9th Cir. 2016); and seeking a prompt meet-and-confer.[1] Over the next two weeks, Advertisers sent additional letters and emails. On May 31, the parties met and conferred and reached impasse.

I. Facebook's IAAP Program Targets Competition By Wiretapping Competitors

On June 9, 2016, Mark Zuckerberg emailed three of the company's top executives a message titled "Snapchat analytics." PX 2255 (PALM-016564834) at 3. According to Zuckerberg:

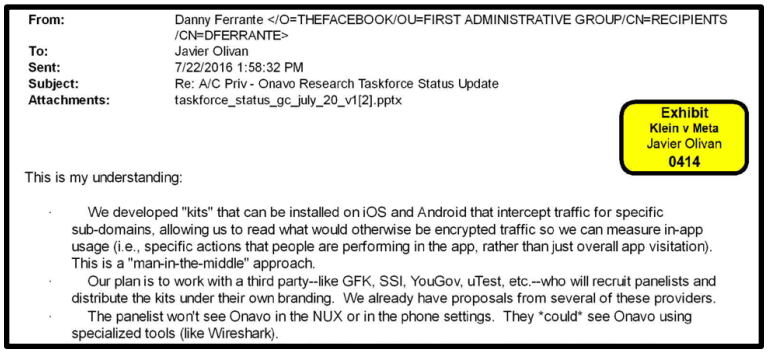
> Whenever someone asks a question about Snapchat, the answer is usually that because their traffic is encrypted we have no analytics about them. . . .
>
> Given how quickly they're growing, it seems important to figure out a new way to get reliable analytics about them. Perhaps we need to do panels or write custom software. You should figure out how to do this.

Id. Javier Olivan, now Facebook's COO, promptly replied, "fully agree[ing] that this was one of the most important market analysis questions we need to answer." *Id.* However, Olivan "ha[d] been looking into this with the onavo team" and the technology to look inside Snapchat's SSL-protected analytics traffic "[wa]s really complicated," likely "requir[ing] legal approval." *Id.* Five minutes later, Olivan forwarded Zuckerberg's email to Facebook's Onavo team, asking for "out of the box thinking" on a task that "is really important." *Id.* at 2. Olivan suggested potentially paying users to "let us install a really heavy piece of software (that could even do man in the middle, etc.)." *Id.* Later that morning, Onavo founder Guy Rosen replied: "we are going to figure out a plan for a lockdown effort during June to bring a step change to our Snapchat visibility. This is an opportunity for our team to shine." *Id.* at 1. Two days later, Olivan forwarded the whole email thread to then-General Counsel Colin Stretch, saying "[w]e should move as fast as possible on this (budget will not be an issue assuming Colin greenlights this type of research on the thread @ Colin

[1] Advertisers stand ready to provide full briefing, exhibits, and/or Advertisers' letters to Facebook at the Court's request.

FILED UNDER SEAL

– correct?). Answering this is really important to give the product teams direction right now." *Id.* On June 17, 2016, the Onavo team created a "kickoff" presentation for the "Ghostbusters project"—an apparent reference to Snapchat's corporate logo, a white ghost on a yellow background. PALM-011630680, at slide 14. This presentation recited Zuckerberg's questions about Snapchat usage, *id.* at slide 22, and analyzed a technological "[s]olution space" that included "SSL bumping," *id*. at slide 3. By July 22, 2016, the Onavo team—under the guidance of in-house counsel—came to a proposed solution for senior leadership. In an email and presentation sent to (among others) Olivan, Rosen, and in-house counsel Dustin St. Clair (who was added "for A/C Priv"), the Onavo team provided details on its "current technical solution," PX 414 (PALM-010629831), at 2: "develop[ing] 'kits' that can be installed on iOS and Android that intercept traffic for specific sub-domains, allowing us to read what would otherwise be encrypted traffic so we can measure in-app usage," *id.* at 1. This was, a Facebook executive told Olivan, "a 'man-in-the-middle' approach," *id.*; *see generally* https://en.wikipedia.org/wiki/Man-in-the-middle_attack.



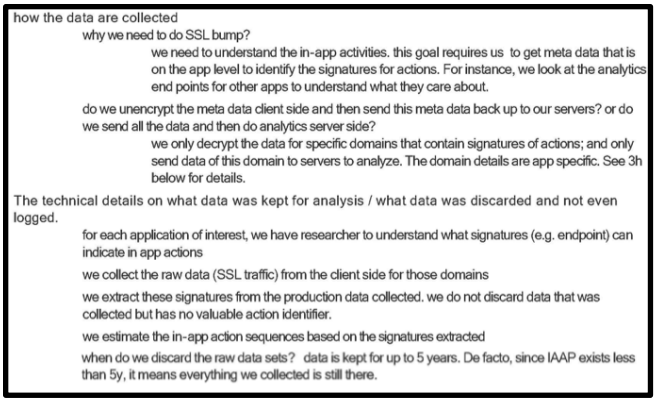
From: Danny Ferrante </O=THEFACEBOOK/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS /CN=DFERRANTE>
To: Javier Olivan
Sent: 7/22/2016 1:58:32 PM
Subject: Re: A/C Priv - Onavo Research Taskforce Status Update
Attachments: taskforce_status_gc_july_20_v1[2].pptx

Exhibit
Klein v Meta
Javier Olivan
0414

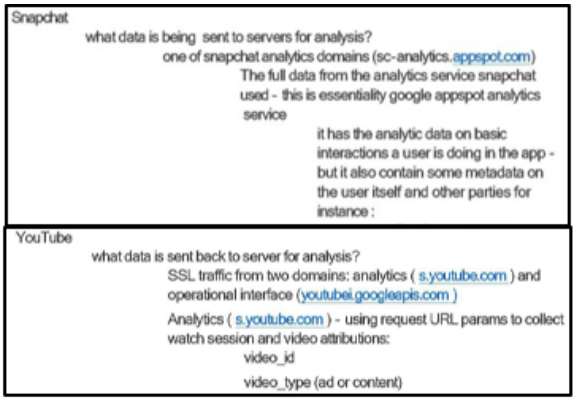
This is my understanding:

- We developed "kits" that can be installed on iOS and Android that intercept traffic for specific sub-domains, allowing us to read what would otherwise be encrypted traffic so we can measure in-app usage (i.e., specific actions that people are performing in the app, rather than just overall app visitation). This is a "man-in-the-middle" approach.
- Our plan is to work with a third party--like GFK, SSI, YouGov, uTest, etc.--who will recruit panelists and distribute the kits under their own branding. We already have proposals from several of these providers.
- The panelist won't see Onavo in the NUX or in the phone settings. They *could* see Onavo using specialized tools (like Wireshark).

Documents and testimony show that this "man-in-the-middle" approach—which relied on technology known as a server-side SSL bump performed on Facebook's Onavo servers—was in fact implemented, at scale, between June 2016 and early 2019. *See* PX 2256 (PALM-012863799) at 1-4. Facebook's SSL bump technology was deployed against Snapchat starting in 2016, then against YouTube in 2017-2018, and eventually against Amazon in 2018. *Id.* at 2-3. The goal of Facebook's SSL bump technology was the company's acquisition, decryption, transfer, and use in competitive decisionmaking of private, encrypted in-app analytics from the Snapchat, YouTube, and Amazon apps, which were supposed to be transmitted over a secure connection between those respective apps and secure servers (sc-analytics.appspot.com for Snapchat, s.youtube.com and youtubei.googleapis.com for YouTube, and *.amazon.com for Amazon). *Id.*



how the data are collected
why we need to do SSL bump?
we need to understand the in-app activities. this goal requires us to get meta data that is on the app level to identify the signatures for actions. For instance, we look at the analytics end points for other apps to understand what they care about.
do we unencrypt the meta data client side and then send this meta data back up to our servers? or do we send all the data and then do analytics server side?
we only decrypt the data for specific domains that contain signatures of actions; and only send data of this domain to servers to analyze. The domain details are app specific. See 3h below for details.
The technical details on what data was kept for analysis / what data was discarded and not even logged.
for each application of interest, we have researcher to understand what signatures (e.g. endpoint) can indicate in app actions
we collect the raw data (SSL traffic) from the client side for those domains
we extract these signatures from the production data collected. we do not discard data that was collected but has no valuable action identifier.
we estimate the in-app action sequences based on the signatures extracted
when do we discard the raw data sets? data is kept for up to 5 years. De facto, since IAAP exists less than 5y, it means everything we collected is still there.



Snapchat
what data is being sent to servers for analysis?
one of snapchat analytics domains (sc-analytics.appspot.com)
The full data from the analytics service snapchat used - this is essentiality google appspot analytics service
it has the analytic data on basic interactions a user is doing in the app - but it also contain some metadata on the user itself and other parties for instance :

YouTube
what data is sent back to server for analysis?
SSL traffic from two domains: analytics (s.youtube.com) and operational interface (youtubei.googleapis.com)
Analytics (s.youtube.com) - using request URL params to collect watch session and video attributions:
video_id
video_type (ad or content)

In order to SSL bump Snapchat—and later YouTube and Amazon—Facebook employees created custom client- and server-side code based on Onavo's VPN proxy app and server stack. PX 1205

at 1-4. This code, which included a client-side "kit" that installed a "root" certificate on Snapchat users' (and later, YouTube and Amazon users') mobile devices, *see* PX 414 at 6, PX 26 (PALM-011683732) ("we install a root CA on the device and MITM all SSL traffic"), also included custom server-side code based on "squid" (an open-source web proxy) through which Facebook's servers created fake digital certificates to impersonate trusted Snapchat, YouTube, and Amazon analytics servers to redirect and decrypt secure traffic from those apps for Facebook's strategic analysis, *see* PX 26 at 3-4 (Sep. 12, 2018: "Today we are using the Onavo vpn-proxy stack to deploy squid with ssl bump the stack runs in edge on our own hosts (onavopp and onavolb) with a really old version of squid (3.1)."); *see generally* http://wiki.squid-cache.org/Features/SslBump.

The intended and actual result of this program was to harm competition, including Facebook's then-nascent Social Advertising competitor Snapchat. Facebook's own documents credit its "Snapchat In-App Panel" with "inform[ing] internal product development" and "[i]ncreas[ing] leadership understanding of Snapchat use cases and the need for different Facebook products to address different Snapchat use cases." PX 20 (PALM-016175119). As one Facebook strategist put it, "SC's struggles as of late due to competition are likely connected to product efforts I have informed via my [Onavo] analysis." *Id.* As a Snap executive testified, Facebook's IAAP-informed product redesigns "hamper[ed] Snap's ability to sell ads." Levenson Dep. 50:12-22.

Between June 2016 and May 2019, Facebook's lawyers were near-constantly involved in the design, deployment, and expansion of the company's IAAP program. Facebook's then-General Counsel was brought in from the outset to "greenlight the type of research on this thread." PX 2255 at 1. Associate General Counsel Dustin St. Clair was involved in the July 2016 Onavo Research Taskforce analysis explaining the final "technical solution" to senior management, PX 414 at 2, then involved again—along with ***approximately 41 other lawyers***—in a January 2019 "IAAP Technical Analysis" document to evaluate whether to continue the program in the face of press scrutiny about Onavo, PX 2256 at 9-10. A September 2018 discussion about "context on IAAP and MITM" stated that the program was "closely monitored" by lawyers in Facebook's "Privacy XFN" team, PX 26 at 3, and was "approved by legal for sure," *id.* at 3-4.

II. Facebook's IAAP Program Violated the Wiretap Act[2]

18 U.S.C. § 2511(1)(a) criminalizes "intentionally intercept[ing] . . . any electronic communications," and subsection (d) of the same statute criminalizes "us[ing]" such intercepted communications. Facebook's IAAP program conduct squarely meets the statutory proscriptions in subsections (a) and (d), including as to "person," "intercept," "intentionally," and "use" within the meaning of the statute. *See generally* PROSECUTING COMPUTER CRIMES, Computer Crime and Intellectual Property Section Criminal Division, U.S. Dep't of Justice (2d ed.) (2010), at 59-87.

Moreover, Facebook's intentional interception of SSL-protected analytics traffic from Snapchat, YouTube, and Amazon did not fall within any statutory exception or defense. In particular, Facebook did not have the consent of Snapchat to intercept its encrypted analytics traffic, and it intercepted this traffic for avowedly tortious purposes, *see* 18 U.S.C. § 2511(2)(d), including to intentionally interfere with Snap, Inc.'s contractual relations with its app users, *see* https://snap.com/en-US/terms (prohibiting all sorts of behaviors that Facebook's IAAP program solicited and paid Snapchat users to engage in).

[2] Advertisers provided Facebook with a six-page version of this analysis, and would be happy to provide a lengthier analysis to the Court if the Court desires it.

FILED UNDER SEAL

Respectfully submitted,

By: *Brian J. Dunne*
On Behalf of Interim Co-Lead Counsel for the Advertiser Classes

SCOTT+SCOTT ATTORNEYS AT LAW LLP

/s/ Amanda F. Lawrence
Amanda F. Lawrence (*pro hac vice*)
alawrence@scott-scott.com
Patrick J. McGahan (*pro hac vice*)
pmcgahan@scott-scott.com
Michael P. Srodoski (*pro hac vice*)
msrodoski@scott-scott.com
156 South Main Street, P.O. Box 192
Colchester, CT 06415
Tel.: (860) 537-5537

Patrick J. Coughlin (CA 111070)
pcoughlin@scott-scott.com
Carmen A. Medici (CA 248417)
cmedici@scott-scott.com
Hal D. Cunningham (CA 243048)
hcunningham@scott-scott.com
Daniel J. Brockwell (CA 335983)
dbrockwell@scott-scott.com
600 W. Broadway, Suite 3300
San Diego, CA 92101
Tel.: (619) 233-4565

Patrick J. Rodriguez (*pro hac vice*)
prodriguez@scott-scott.com
230 Park Avenue, 17th Floor
New York, NY 10169
Tel.: (212) 223-6444

BATHAEE DUNNE LLP

/s/ Yavar Bathaee
Yavar Bathaee (CA 282388)
yavar@bathaeedunne.com
Andrew C. Wolinsky (CA 345965)
awolinsky@bathaeedunne.com
Adam Ernette (*pro hac vice*)
aernette@bathaeedunne.com
Priscilla Ghita (*pro hac vice*)
pghita@bathaeedunne.com
Chang Hahn (*pro hac vice*)
chahn@bathaeedunne.com
445 Park Avenue, 9th Floor
New York, NY 10022
(332) 322-8835

Brian J. Dunne (CA 275689)
bdunne@bathaeedunne.com
Edward M. Grauman (*pro hac vice*)
egrauman@bathaeedunne.com
Andrew M. Williamson (CA 344695)
awilliamson@bathaeedunne.com
901 S. MoPac Expressway
Barton Oaks Plaza I, Suite 300
Austin, TX 78746
(213) 462-2772

Allison Watson Cross (CA 328596)
across@bathaeedunne.com
3420 Bristol St., Ste 600
Costa Mesa, CA 92626-7133

Interim Co-Lead Counsel for the Advertiser Classes

FILED UNDER SEAL

FILER ATTESTATION

I am the ECF user who is filing this document. Pursuant to Civil L.R. 5-1(h)(3), I hereby attest that each of the other signatories have concurred in the filing of the document.

Dated: May 31, 2023

By: */s/ Brian J. Dunne*
Brian J. Dunne